

Palo Alto Networks®
Guía del administrador de Panorama

Panorama 5.1

Información de contacto

Sede de la empresa:

Guía del administrador

3300 Olcott Street

Santa Clara, CA 95054

http://www.paloaltonetworks.com/contact/contact/

Acerca de esta guía

En esta guía se explica cómo configurar y utilizar Panorama para conseguir una gestión centralizada; está dirigida a administradores que buscan un marco básico para configurar rápidamente el dispositivo virtual de Panorama o el dispositivo M-100 y conseguir la administración centralizada de los cortafuegos de Palo Alto Networks.

Si dispone de un dispositivo M-100, en esta guía se asume que ha completado el montaje en rack del dispositivo M-100.

Para obtener más información, consulte las siguientes fuentes:

- Guía del administrador de Palo Alto Networks: para obtener instrucciones sobre cómo configurar las funciones del cortafuegos. La guía del administrador de Palo Alto Networks también le ayuda con los aspectos relacionados con la configuración de Panorama que son parecidos a los del cortafuegos pero que no están cubiertos en esta guía.
- https://live.paloaltonetworks.com: para acceder a bases de conocimientos, a un completo conjunto de documentación, foros de discusión y vídeos.
- https://support.paloaltonetworks.com: para ponerse en contacto con el equipo de asistencia técnica, obtener información sobre los programas de asistencia técnica o gestionar la cuenta o los dispositivos.

Para enviar sus comentarios sobre la documentación, diríjase a: documentation@paloaltonetworks.com.

Palo Alto Networks, Inc.
www.paloaltonetworks.com

Número de pieza 810-000177-00B

Contenido

Descripción general de Panorama 1

Acerca de Panorama 2

Plataformas de Panorama 3

Información sobre la gestión de la implementación y la configuración centralizada 4
- Cambio de contexto: dispositivo o Panorama 4
- Plantillas 4
- Grupos de dispositivos 5

Acerca de la creación centralizada de logs y de informes 8
- Opciones de creación de logs 8
- Recopiladores gestionados y grupos de recopiladores 9
- Uso de varios recopiladores de logs en un grupo de recopiladores 9
- Informes centralizados 11

Acerca del control de acceso en base al rol 12
- Funciones administrativas 12
- Perfiles y secuencias de autenticación 13
- Dominios de acceso 13
- Autenticación administrativa 13

Implementaciones recomendadas de Panorama 15
- Panorama para gestión centralizada y creación de informes. 15
- Panorama en una arquitectura de recopilación de logs distribuida. 16

Planificación de su implementación. 17

Implementación Panorama: Lista de comprobación de descripción general de tareas. 19

Configuración de Panorama 21

Configuración del dispositivo virtual de Panorama 22
- Requisitos 22
- Instalación de Panorama en el servidor ESX(i) 23
- Realización de la configuración inicial 25
- Ampliación de la capacidad de almacenamiento del log en el dispositivo virtual de Panorama 27

Configuración del dispositivo M-100 30
- Realización de la configuración inicial 31
- Configuración del dispositivo M-100 en modo de recopilación de logs 33
- Aumento de la capacidad de almacenamiento en el dispositivo M-100 35

Migración de un dispositivo virtual de Panorama a un dispositivo M-100 37
- Requisitos 37
- Consideraciones de planificación 38
- Realización de la migración 39
- Reanudación de la gestión de dispositivos. 41

Instalación de licencias 42
- Registro de Panorama 42
- Activación/recuperación de licencias 43

Instalación de las actualizaciones de contenido y software de Panorama 45

Navegación en la interfaz de usuario de Panorama 47
Navegación en la interfaz web 47
Inicio de sesión en la interfaz web 48
Inicio de sesión en la CLI 49

Configuración del acceso administrativo 50
Creación de una cuenta administrativa 50
Definición de los dominios de acceso 52
Creación de un perfil de autenticación 53
Definición de una secuencia de autenticación 54
Configuración de la autenticación administrativa 54

Gestión de cortafuegos y recopilación de logs 61

Gestión de sus cortafuegos 62
Adición de dispositivos gestionados 62
Creación de grupos de dispositivos 64
Creación de plantillas 71
Configuración de los cortafuegos para reenviar logs a Panorama 76
Compilación de cambios en Panorama 81
Modificación de los valores predeterminados de almacenamiento en búfer y reenvío de logs 82
Uso de Panorama para configurar dispositivos gestionados: ejemplo 84

Habilitación de logs 93

Implementación de actualizaciones de software y gestión de licencias 101

Sustitución de un dispositivo gestionado por un nuevo dispositivo 104
Antes de comenzar 104
Restablecimiento de la configuración en el nuevo dispositivo 106

Transición de un dispositivo a una gestión central 109

Supervisión de la actividad de red 111

Uso de Panorama para lograr visibilidad 112
Supervisión de la red con el ACC y Appscope 112
Análisis de datos de log 115
Generación de informes 115

Caso de uso: supervisión de aplicaciones mediante Panorama 118

Caso de uso: uso de Panorama para responder a un incidente 122

Alta disponibilidad de Panorama 127

Descripción general de la alta disponibilidad 128
Activadores de conmutación por error 129
Consideraciones sobre el registro en HA 130
Prioridad y conmutación por error 131
¿Qué configuración no está sincronizada entre los peers de HA? 132

Configuración de un clúster en alta disponibilidad de Panorama 134
Configuración de alta disponibilidad en Panorama 134
Verificación de conmutación por error 137
Cambio de prioridad para reanudar los logs en NFS 137

Actualización de Panorama en alta disponibilidad 139

Administración de Panorama 141

Gestión de las copias de seguridad de la configuración 142
Programación de la exportación de los archivos de configuración 143
Gestión de las copias de seguridad de configuración de Panorama 144
Configuración del número de copias de seguridad almacenadas en Panorama 145
Carga de una copia de seguridad de configuración en un dispositivo gestionado 145

Comparación de cambios en la configuración 146

Restricción de acceso a los cambios de configuración 147
Tipos de bloqueos 147
Ubicaciones para aplicar un bloqueo 148
Aplicación de un bloqueo 148
Visualización de los portadores de bloqueo actuales 148
Habilitación de la adquisición automática del bloqueo de compilación 149
Eliminación de un bloqueo. 149

Adición de logotipos personalizados 150

Visualización del historial de finalización de tareas. 151

Reasignación de cuotas de almacenamiento de logs 152

Supervisión de Panorama 154
Configuración de alertas de correo electrónico 155
Configuración del acceso SNMP 156

Reinicio o cierre de Panorama 160

Generación de archivos de diagnóstico 161

Configuración de perfiles de contraseña y complejidad de contraseña 162

Sustitución del disco virtual en un dispositivo virtual de Panorama 163

Solución de problemas 165

¿Por qué falla la compilación de plantillas? 165
¿Por qué ejecuta Panorama una comprobación de integridad del sistema de archivos? 166
¿Hay una conexión distinta para reenviar los logs a Panorama?. 166
¿Por qué la capacidad de almacenamiento de logs del grupo de recopiladores indica 0 MB?. 167
¿Por qué está Panorama en un estado suspendido? 167
¿Dónde puedo ver el estado de la tarea? 167

1 Descripción general de Panorama

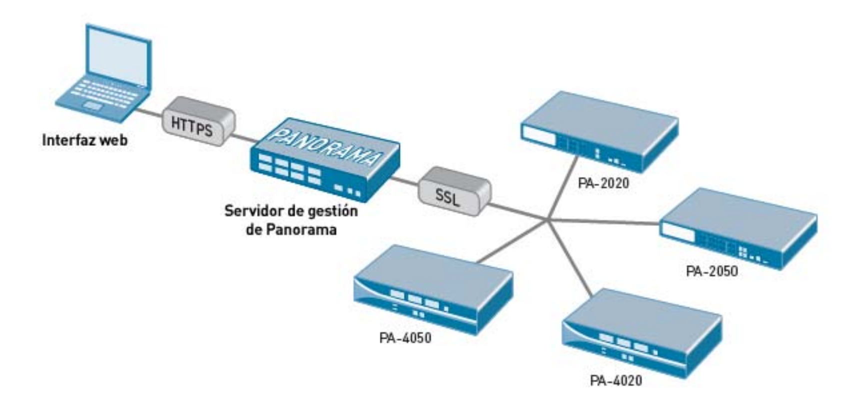
Panorama ofrece gestión centralizada y visibilidad de múltiples cortafuegos de última generación de Palo Alto Networks. Le permite supervisar todas las aplicaciones, usuarios y contenidos que atraviesan la red desde una ubicación, y emplear esta información para crear políticas de activación de aplicaciones que protejan y controlen toda la red. Si se usa Panorama para gestionar de forma centralizada las políticas y dispositivos es posible aumentar la eficiencia operativa a la hora de gestionar y mantener una red distribuida de cortafuegos.

Las siguientes secciones describen Panorama y ofrecen directrices para planificar su implementación de Panorama:

- Acerca de Panorama
- Plataformas de Panorama
- Información sobre la gestión de la implementación y la configuración centralizada
- Acerca de la creación centralizada de logs y de informes
- Acerca del control de acceso en base al rol
- Implementaciones recomendadas de Panorama
- Planificación de su implementación
- Implementación Panorama: Lista de comprobación de descripción general de tareas

Acerca de Panorama

Panorama ofrece una gestión centralizada de los cortafuegos de última generación de Palo Alto Networks, tal y como se muestra en la siguiente ilustración:



Panorama le permite configurar, gestionar y supervisar de forma efectiva sus cortafuegos de Palo Alto Networks mediante una supervisión central con control local, según sea necesario. Los tres puntos fundamentales en los que Panorama añade valor son:

- Configuración e implementación centralizadas: puede simplificar la gestión central e implementar rápidamente los cortafuegos de su red si utiliza Panorama para las fases previas a la implementación de los cortafuegos. Puede reunir los dispositivos en grupos, crear plantillas para aplicar una configuración de dispositivos y red base y usar grupos de dispositivos para administrar globalmente políticas locales y compartidas. Consulte Información sobre la gestión de la implementación y la configuración centralizada.
- Logs agregados con perspectiva central para análisis e informes: recopile información de actividades en los cortafuegos gestionados de la red y analice, investigue y cree informes de forma centralizada sobre los datos. Esta exhaustiva vista del tráfico de la red, la actividad del usuario y los riesgos asociados le permiten responder a posibles amenazas usando la rica gama de políticas para activar de forma segura las aplicaciones de su red. Consulte Acerca de la creación centralizada de logs y de informes.
- Administración distribuida: le permite delegar o restringir el acceso a políticas y configuraciones de dispositivos globales y locales. Consulte Acerca del control de acceso en base al rol para saber cómo delegar los niveles apropiados de acceso para la administración distribuida.

Panorama está disponible en dos plataformas: un dispositivo virtual y un dispositivo de hardware dedicado. Para obtener más información, consulte Plataformas de Panorama.

Plataformas de Panorama

Panorama está disponible en dos plataformas, cada una de las cuales admite licencias de gestión de dispositivos para gestionar hasta 25 dispositivos, hasta 100 dispositivos o hasta 1000 dispositivos:

- **Dispositivo virtual de Panorama**: el dispositivo virtual de Panorama se instala en un servidor VMware. Permite una instalación sencilla y facilita la consolidación de los sitios que necesitan un dispositivo de gestión virtual. También admite la integración con un sistema de archivos de red (NFS) para una mayor capacidad de almacenamiento y de conservación de logs (> 2 TB).

  El dispositivo virtual de Panorama es ideal para entornos con menos de 10 cortafuegos y tasas de log inferiores a 10 000 logs/segundo.

- **Dispositivo M-100**: dispositivo hardware dedicado para implementaciones a gran escala. En entornos con elevados requisitos de conservación de logs y altas tasas de log, esta plataforma permite ampliar su infraestructura de recopilación de logs. El dispositivo admite la configuración en RAID 1 para permitir la protección contra fallos del disco y la configuración predeterminada incluye dos unidades de 1 TB; con lo que, si se le suman los pares de RAID adicionales, el dispositivo M-100 puede admitir hasta 4 TB de almacenamiento de log.

  El dispositivo M-100 permite separar la función de gestión central de la función de recopilación de logs mediante los siguientes modos de implementación:

  – **Modo Panorama**: El dispositivo realiza tanto la función de gestión central como la de recopilación de logs. Es el modo predeterminado.

  – **Modo de recopilación de logs**: El dispositivo actúa como recopilador de logs dedicado, que puede gestionarse ya sea mediante un dispositivo M-100 en modo Panorama o mediante un dispositivo virtual de Panorama.

    Cuando se implementa en modo de recopilación de logs, el dispositivo no tiene una interfaz web, sino que el acceso administrativo solo es a través de la CLI.

La plataforma se elegirá en función de sus necesidades de un dispositivo virtual, el número de cortafuegos de Palo Alto Networks que pretenda gestionar y los requisitos de recopilación de logs tal y como se detalla en la siguiente tabla:

Consideraciones	VMware	M-100	
	Dispositivo virtual de Panorama	Modo Panorama	Arquitectura de logs distribuida con recopiladores de logs dedicados
Número de dispositivos gestionados	10 cortafuegos o menos	Hasta 100 cortafuegos	Hasta 1000 cortafuegos
IP de recopilación de logs	<10 000 logs/segundo	<10 000 logs/segundo	>10 000 logs/segundo (Máx. 50 000 logs/seg por recopilador)

Información sobre la gestión de la implementación y la configuración centralizada

Panorama usa *Grupos de dispositivos* y *Plantillas* para agrupar los dispositivos en conjuntos más pequeños y lógicos que requieren una configuración similar. Todos los elementos de configuración, políticas y objetos de los cortafuegos gestionados pueden gestionarse de forma centralizada en Panorama mediante grupos de dispositivos y plantillas. Además de gestionar la configuración y las políticas, Panorama le permite gestionar a nivel central las licencias, el software y las actualizaciones de contenido asociadas, como los clientes SSL-VPN, los agentes GlobalProtect y las actualizaciones de contenido dinámico (aplicaciones, amenazas, WildFire y antivirus).

Cambio de contexto: dispositivo o Panorama

La interfaz web de Panorama le permite cambiar entre una vista centrada en Panorama a un vista centrada en los dispositivos mediante un *cambio de contexto*. Puede optar entre gestionar el dispositivo de forma centralizada con Panorama y cambiar el contexto a un dispositivo gestionado específico para configurar el dispositivo usando su interfaz de usuario. Las similitudes entre la interfaz de usuario en los cortafuegos gestionados y Panorama le permiten cambiar sin problemas entre las dos interfaces para administrar y supervisar los dispositivos según sea necesario.

Si ha configurado dominios de acceso para restringir el acceso administrativo a dispositivos gestionados específicos, la interfaz de usuario de Panorama solo muestra los dispositivos/características para las que tiene permisos el administrador que ha iniciado sesión.

Plantillas

Las plantillas se usan para configurar los ajustes necesarios para que los cortafuegos gestionados operen en la red. Le permiten definir una configuración base común mediante las pestañas **Red** y **Dispositivo** de Panorama. Usando plantillas, se puede gestionar, por ejemplo, la interfaz y la configuración de zona, los perfiles de servidor para la creación de logs y el acceso a SNMP o los perfiles de red para controlar el acceso a zonas y cortafuegos de IKE. Cuando agrupe dispositivos para definir la configuración de la plantilla, agrupe aquellos que sean parecidos en cuanto a modelo de hardware y necesiten acceder a recursos de red similares, como cortafuegos y servidores Syslog.

Mediante las plantillas, puede aplicar una configuración base común limitada en un grupo de dispositivos y, a continuación, configurar el resto de ajustes manualmente en el dispositivo. Otra posibilidad es aplicar una configuración base común mayor y, a continuación, sobrescribir la configuración de la plantilla en el dispositivo para adaptarlo a cambios específicos. Cuando sobrescribe un ajuste en el dispositivo, este se guarda en la configuración local del mismo y la plantilla de Panorama deja de gestionarlo. Sin embargo, puede usar Panorama para aplicar la configuración de la plantilla en el dispositivo o restaurar la configuración de la plantilla en el dispositivo. Por ejemplo, puede definir un servidor NTP común en la plantilla y sobrescribir la configuración del servidor NTP en el dispositivo para adaptar la zona horaria local en el dispositivo. Si decide restaurar la configuración de la plantilla más adelante, puede deshacer fácilmente los cambios locales que ha implementado en el dispositivo.

Las plantillas no se pueden utilizar para definir un cambio de estado operativo como el modo FIPS ni para habilitar el modo de VSYS múltiple en los cortafuegos. Para obtener más información, consulte Acciones para las que no se pueden utilizar las plantillas.

Grupos de dispositivos

Para usar Panorama eficazmente, debe agrupar los cortafuegos de la red en unidades lógicas denominadas *grupos de dispositivos*. Un grupo de dispositivos permite realizar las agrupaciones basadas en la segmentación de la red, la ubicación geográfica o en caso de que sea necesario implementar configuraciones de política similares. Un grupo de dispositivos puede incluir cortafuegos físicos, virtuales y/o sistemas virtuales. De forma predeterminada, todos los dispositivos gestionados pertenecen al grupo de dispositivos *Compartido* de Panorama.

Los grupos de dispositivos permiten la gestión central de políticas y objetos mediante las pestañas **Políticas** y **Objetos** de Panorama. Los objetos son elementos de configuración a los que se hace referencia en las políticas. Algunos de los objetos de los que hacen uso las políticas de cortafuegos son: Direcciones IP, categorías de URL, perfiles de seguridad, usuarios, servicios y aplicaciones.

Utilizando los grupos de dispositivos puede crear objetos compartidos u objetos específicos de un grupo de dispositivos y, a continuación, utilizar estos objetos para crear una jerarquía de reglas (y bases de reglas) para indicar cómo deben gestionar los cortafuegos gestionados el tráfico entrante y saliente. Por ejemplo, una política de uso corporativa aceptable se podría definir como un conjunto de políticas compartidas. A continuación, para que solo las oficinas regionales accedan al tráfico de peer-a-peer como bittorrent, puede crear una regla de seguridad como política compartida y aplicarla a las oficinas regionales o convertirla en una regla de grupo de dispositivos que se aplique a las oficinas regionales. Consulte Uso de Panorama para configurar dispositivos gestionados: ejemplo.

Acerca de las políticas

Los grupos de dispositivos son una forma de implementar un método de capa para gestionar políticas en una red de cortafuegos gestionados. El método de capa permite la implementación de políticas corporativas de forma centralizada, como las *políticas compartidas*, junto con *políticas específicas de grupos de dispositivos*y políticas administradas *localmente* en el dispositivo.

Tanto las políticas compartidas como las específicas de un grupo de dispositivos le permiten crear reglas previas y reglas posteriores para gestionar todas las bases de reglas desde una ubicación central: seguridad, NAT, QoS, reenvío basado en políticas, descifrado, cancelación de aplicación, portal cautivo y protección DoS.

- **Reglas previas**: reglas que se añaden al principio del orden de reglas y se evalúan en primer lugar. Puede utilizar las reglas previas para aplicar la política de uso aceptable para una organización; por ejemplo, para bloquear el acceso a categorías de URL específicas o permitir el tráfico DNS a todos los usuarios. Las reglas previas pueden ser de dos tipos: Reglas previas compartidas, que se comparten en todos los dispositivos gestionados y grupos de dispositivos, y reglas previas de grupo de dispositivos, específicas para un grupo de dispositivos.

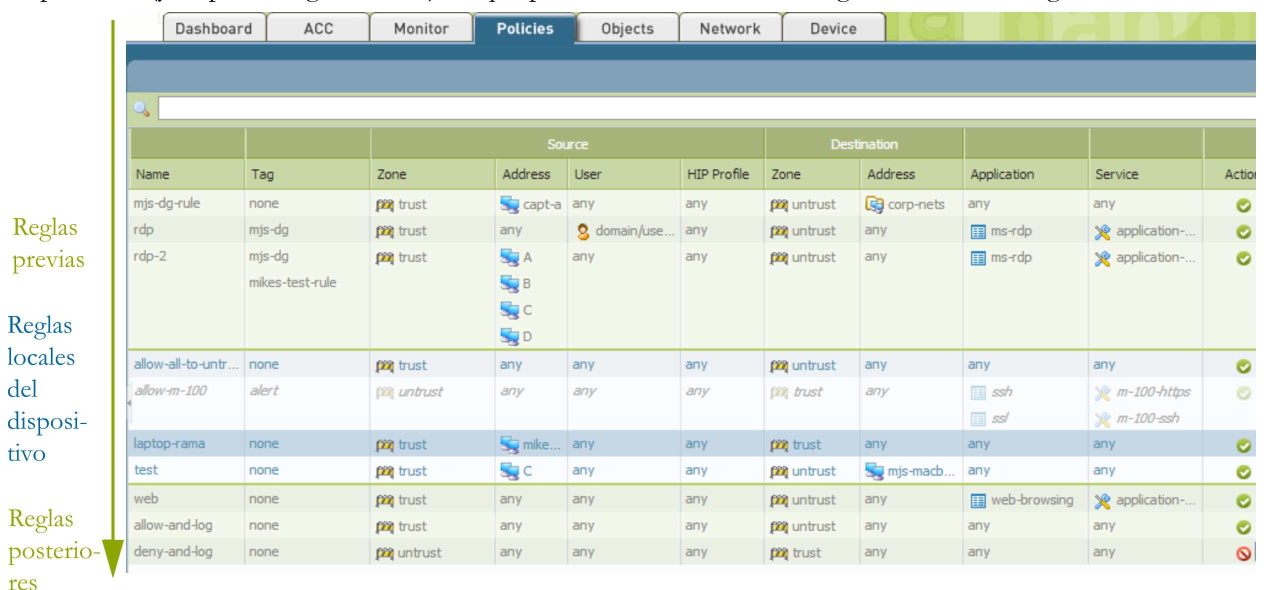
- **Reglas posteriores**: reglas que se añaden al final del orden de reglas y que se evalúan después de las reglas previas y de las reglas definidas localmente en el dispositivo. Las reglas posteriores suelen incluir reglas para impedir el acceso al tráfico basado en App-ID, ID de usuario o servicio. Como las reglas previas, las posteriores también pueden ser de dos tipos: Reglas posteriores compartidas, que se comparten en todos los dispositivos gestionados y grupos de dispositivos, y reglas posteriores de grupo de dispositivos, específicas para un grupo de dispositivos.

El orden de evaluación de las reglas es:



Cuando el tráfico coincide con una regla de política, la acción definida se activa y se descartan todas las políticas siguientes.

Este método de capas con las políticas crea una jerarquía de reglas en la cual las políticas locales se sitúan entre las reglas previas y las posteriores y se pueden editar cambiando al contexto de cortafuegos local o accediendo localmente al dispositivo. Esta cascada de reglas se marca visualmente para cada grupo de dispositivos (y dispositivo gestionado), lo que permite revisarlas entre un gran número de reglas.



Las reglas previas y las posteriores transferidas desde Panorama se pueden ver en los cortafuegos gestionados, pero solo se pueden editar en Panorama. Las reglas de dispositivos locales las puede editar el administrador local o un administrador de Panorama que haya cambiado a un contexto de cortafuegos local.

Acerca de los objetos

Los objetos son elementos de configuración a los que se hace referencia en las políticas. Algunos de los objetos de los que hacen uso las políticas de cortafuegos son: Direcciones IP, categorías de URL, perfiles de seguridad, usuarios, servicios y aplicaciones. Como lo objetos se pueden reutilizar en varias políticas, la creación de *objetos compartidos* u *objetos de grupo de dispositivos* reduce la duplicación de estos elementos de configuración. For example, creating shared address objects and address groups or shared service objects and service groups allows you to create one instance of the object and reference it in any rulebase to manage the firewalls across multiple device groups. Como los objetos compartidos se definen una vez pero se utilizan muchas otras, reducen la carga administrativa y mantienen la coherencia y la precisión en cualquier lugar donde se utilice el objeto compartido.

Tanto los objetos compartidos como los objetos de grupo de dispositivos se pueden utilizar en las reglas previas, reglas posteriores y reglas definidas localmente en un dispositivo. Cuando crea un objeto en Panorama, puede configurar el comportamiento si:

- El objeto del grupo de dispositivos tiene prioridad sobre un objeto compartido, cuando ambos objetos tienen el mismo nombre. De forma predeterminada, el objeto compartido tiene prioridad. Este comportamiento garantiza que un objeto compartido siempre sustituya a un objeto de grupo de dispositivos con el mismo nombre.

  Sin embargo, si un dispositivo tiene un objeto creado localmente con el mismo nombre que un objeto compartido u objeto de grupo de dispositivos transferido desde Panorama, se producirá un fallo de compilación.

- Todos los objetos compartidos u objetos de grupo de dispositivos definidos en Panorama se aplican en los dispositivos gestionados. De forma predeterminada, todos los objetos (tanto si se hace referencia a ellos en las políticas como si no) se transfieren a los dispositivos gestionados.

Acerca de la creación centralizada de logs y de informes

Panorama permite agregar datos de todos los cortafuegos gestionados y conseguir visibilidad en todo el tráfico de su red. También proporciona un seguimiento auditado para todas las modificaciones de políticas y cambios de configuración realizados en los dispositivos gestionados.

El Centro de comando de aplicación (ACC) de Panorama ofrece un panel único para la creación unificada de informes de todos los cortafuegos; le permite realizar análisis, investigaciones e informes de forma centralizada sobre el tráfico de red e incidentes de seguridad. En Panorama, puede ver logs y generar informes de logs reenviados a Panorama o a los recopiladores de logs gestionados, si están configurados, o consultar los dispositivos gestionados directamente. Por ejemplo, puede generar informes sobre tráfico, amenazas o actividad de los usuarios en la red gestionada basada en logs almacenados en Panorama (y en recopiladores de logs gestionados) o accediendo a los logs almacenados localmente en los dispositivos gestionados.

Si elige no configurar los cortafuegos gestionados para que se reenvíen logs a Panorama, puede programar la ejecución de informes en cada uno de los cortafuegos gestionados y reenviar los resultados a Panorama para obtener una vista combinada de la actividad del usuario y el tráfico de red. Aunque esta vista no proporciona un desglose detallado de datos y actividades específicos, sí permite ver los informes de forma unificada.

Opciones de creación de logs

Tanto el dispositivo virtual de Panorama como el dispositivo M-100 pueden realizar la recopilación de logs para aquellos que se reenvían desde los dispositivos gestionados. Las opciones de creación de logs varían en cada plataforma.

- **En un dispositivo virtual de Panorama** hay tres opciones para la creación de logs: utilizar los 10 GB de espacio de almacenamiento interno asignados para la creación de logs tan pronto como instale el dispositivo virtual, añadir un disco virtual que pueda admitir hasta 2 TB de almacenamiento o montar un almacén de datos del sistema de archivos de red (NFS), donde determinar la capacidad de almacenamiento asignada a la creación de logs.

- **En el dispositivo M-100** la configuración de envío predeterminada incluye discos de 1 TB en un par de RAID, que puede aumentar a un almacenamiento RAID de 4 TB. Cuando el dispositivo M-100 se encuentre en modo Panorama, podrá habilitar los discos RAID y utilizarlos como recopilador de logs predeterminado. Con el dispositivo M-100 en modo de recopilación de logs, debe utilizar Panorama para asignar los dispositivos a aquellos del recopilador de logs. En una implementación con varios dispositivos de recopilación de logs, Panorama consulta todos los recopiladores de logs gestionados para generar un vista agregada de informes de tráfico e informes cohesivos.

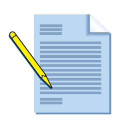
  Para una ampliación fácil, empiece con un único Panorama y añada recopiladores de logs específicos progresivamente, conforme aumenten las necesidades.

Recopiladores gestionados y grupos de recopiladores

Un recopilador de logs es un dispositivo M-100 configurado para funcionar en modo de *recopilación de logs*. Es un dispositivo de recopilación de logs especializado que se ha configurado y gestionado usando Panorama y que por lo tanto se denomina "recopilador gestionado". Puede estar gestionado por un dispositivo M-100 en modo Panorama o por un dispositivo virtual de Panorama. Cuando se añade como recopilador gestionado y se conecta a Panorama, el recopilador de logs se puede administrar usando la interfaz web de Panorama. De lo contrario, el acceso administrativo al recopilador de logs solo está disponible a través de la CLI utilizando la cuenta del usuario administrativo predeterminado (*admin*). No están admitidas otras cuentas de usuario administrativo.

Un grupo de recopiladores es uno o varios dispositivos M-100 que funcionan como una unidad de recopilación de logs lógica sencilla. Los logs se distribuyen uniformemente entre todos los discos de un recopilador de logs y en todos los miembros de un grupo de recopiladores. El reparto uniforme de los logs en todos los discos y recopiladores de logs maximiza el uso del espacio de almacenamiento disponible. Cada Panorama puede gestionar hasta 16 grupos de recopiladores. Para gestionar un recopilador de logs, debe añadirlo a un grupo de recopiladores. Aunque un grupo de recopiladores puede contener varios recopiladores de logs, Palo Alto Networks recomienda ubicar un único recopilador de logs en un grupo de recopiladores a no ser que se necesite más de 4 TB de espacio de almacenamiento en un grupo de recopiladores.

La configuración del grupo de recopiladores especifica qué cortafuegos gestionados pueden enviar logs a los recopiladores de logs del grupo. Después de que los recopiladores de logs se configuren y los cortafuegos se habiliten para reenviar logs, todos los dispositivos reenvían sus logs al recopilador de logs asignado.



Si usa Panorama para gestionar cortafuegos que se ejecuten tanto en la versión 5.0 de PAN-OS como en una versión anterior, tenga en cuenta los siguientes requisitos de compatibilidad:

- Solo los dispositivos que ejecutan PAN-OS v 5.0 pueden enviar logs a un recopilador de logs específico (dispositivo M-100 configurado en el modo de recopilación de logs).

- Los dispositivos que ejecutan versiones de PAN-OS anteriores a la 5.0a pueden enviar logs a un dispositivo virtual de Panorama o a un dispositivo M-100 en el modo Panorama.

Los recopiladores gestionados y los grupos de recopiladores pertenecen a la arquitectura de recopilación de logs distribuida de Panorama. La arquitectura de recopilación de logs distribuida permite una fácil ampliación y un aumento progresivo de los recopiladores de logs específicos conforme crecen las necesidades de creación de logs. El dispositivo M-100 en modo Panorama se puede registrar en su grupo de recopiladores predeterminado y ampliarse después a una arquitectura de recopilación de logs distribuida con uno o varios grupos de recopiladores que incluyen dispositivos M-100 en modo de recopilación de logs.

Uso de varios recopiladores de logs en un grupo de recopiladores

Aunque Palo Alto Networks recomienda situar solo un recopilador de logs en un grupo de recopiladores,en caso de que se necesiten más de 4 TB de capacidad de almacenamiento de logs en un grupo de recopiladores, puede que necesite añadir varios recopiladores de logs al grupo de recopiladores. Puede que un grupo de recopiladores de logs necesite varios recopiladores de logs en los siguientes casos:

- Un cortafuegos único que genere más de 4 TB de logs. Por ejemplo, si un cortafuegos gestionado genera 12 TB de logs, necesitará al menos tres recopiladores de logs en el grupo de recopiladores.

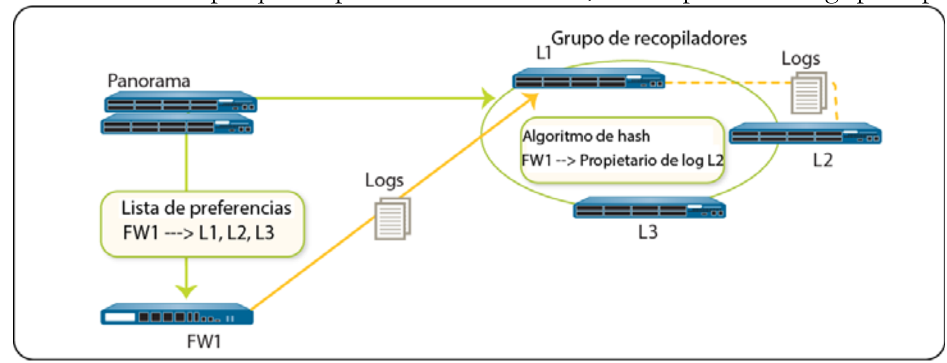
- Un grupo de cortafuegos que reenvíe logs a un grupo de recopiladores y los requisitos de capacidad superen los 4 TB de espacio de almacenamiento.

Si un grupo de recopiladores contiene varios recopiladores de logs, el espacio de almacenamiento disponible se utiliza como unidad lógica única y los logs se distribuyen uniformemente en todos los recopiladores de logs del grupo del recopiladores. La distribución de logs se basa en la capacidad del disco de los recopiladores de logs (que va de 1 a 4 TB, según el número de pares de discos) y un algoritmo de hash que decide dinámicamente qué recopilador de logs posee los logs y escribe en el disco. Aunque Panorama utiliza una lista de preferencias para priorizar la lista de recopiladores de logs a los que puede reenviar logs un cortafuegos gestionado, los logs no tienen por qué estar escritos necesariamente en el primer recopilador de logs especificado en la lista de preferencias.

Por ejemplo, consideremos la siguiente lista de preferencias:

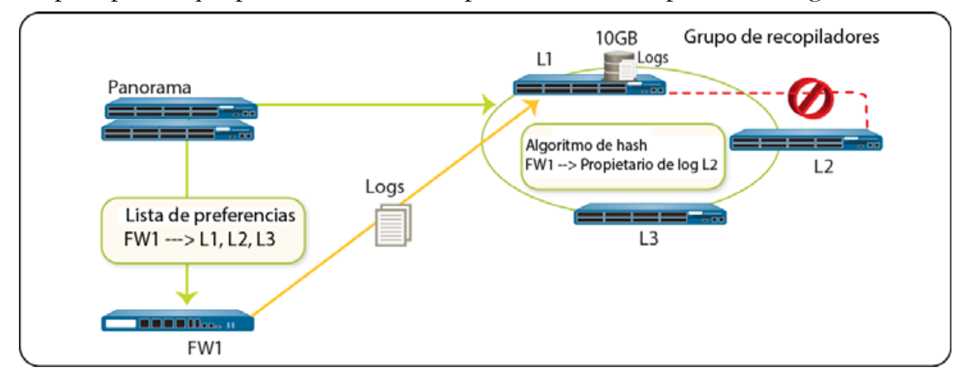
Cortafuegos gestionado	Lista de preferencias de reenvío de logs definida en un grupo de recopiladores
FW1	L1,L2,L3
FW2	L4,L5,L6

Con esta lista, FW1 reenviará logs a L1, su recopilador de logs principal, aunque el algoritmo de hash podría determinar que los logs se escriban en L2. Si no se puede acceder a L2 o este tiene un fallo de bastidor, FW1 no detectará este fallo porque no puede conectarse a L1, su recopilador de logs principal.



En el caso que solo haya un recopilador de logs configurado en un grupo de recopiladores y este falle, el cortafuegos almacena los logs en su HDD/SSD (el espacio de almacenamiento disponible varía según el modelo de hardware) y reanuda el reenvío de logs al recopilador en el lugar donde lo dejó se produjo el fallo tan pronto como se restaure la conectividad.

Cuando hay varios recopiladores de logs en un grupo de recopiladores, el cortafuegos no almacena los logs en el búfer de su almacenamiento local cuando puede conectarse a su recopilador de logs principal. Por lo tanto, FW1 continuará enviando logs a L1. Como L2 no está disponible, el recopilador de logs principal L1 almacena los logs en el búfer de su HDD, que tiene un espacio para logs de 10 GB. Si L2 permanece no disponible y los logs que esperan a L2 superan los 10 GB, L1 sobrescribirá la entradas de logs más antiguas para poder continuar la creación de logs. En este caso, existe el riesgo de que se pierdan logs. Por lo tanto, si se utilizan varios recopiladores de logs en un grupo de recopiladores, asegúrese de contar con un recambio (OSS) o una unidad de espera pasiva que permitan sustituir rápidamente el recopilador de logs si este sufriera algún fallo.



Informes centralizados

Panorama añade logs procedentes de todos los dispositivos gestionados y permite la creación de informes sobre los datos agregados para obtener una visión global del uso de las aplicaciones, la actividad del usuario y los patrones de tráfico de toda la infraestructura de la red. Tan pronto como los cortafuegos se añaden a Panorama, el ACC puede mostrar todo el tráfico que atraviesa su red. Con la creación de informes habilitada, podrá acceder directamente a los detalles específicos sobre la aplicación. haciendo clic en la entrada de un log en el ACC.

Para generar informes, Panorama utiliza dos fuentes: la base de datos local de Panorama y los dispositivos remotos que gestiona. La base de datos de Panorama se refiere al almacenamiento local de Panorama asignado para almacenar tanto logs resumidos como algunos logs detallados. Si dispone de una arquitectura de recopilación de logs distribuida, la base de datos de Panorama incluirá el almacenamiento local en Panorama y todos los recopiladores de logs gestionados. Panorama resume la información (tráfico, aplicaciones, amenazas) recogida de todos los dispositivos gestionados en intervalos de 15 minutos. Usando la base de datos local de Panorama se consiguen unos tiempos de respuesta más rápidos. Sin embargo, si prefiere no reenviar logs a Panorama, Panorama puede acceder directamente al dispositivo remoto y ejecutar informes sobre datos almacenados localmente en los dispositivos gestionados.

Panorama ofrece más de 40 informes predefinidos que se pueden utilizar tal cual o que se pueden personalizar combinando elementos de otros informes para generar informes personalizados y grupos de informes que se pueden guardar. Los informes se pueden generar según se necesiten, con una planificación recurrente, y se puede programar su envío diario por correo electrónico. Estos informes proporcionan información sobre el usuario y el contexto, así que puede hacer corresponder eventos e identificar patrones, tendencias y áreas potenciales de interés. Con el método integrado de creación de logs e informes, el ACC permite la correlación de entradas de varios logs relacionados con el mismo evento.

Acerca del control de acceso en base al rol

El control de acceso en base al rol le permite especificar los privilegios y responsabilidades correspondientes a cada usuario administrativo. En Panorama, puede definir las cuentas administrativas con funciones, perfiles o *dominios de acceso* específicos para regular el acceso a determinadas funciones de Panorama y los dispositivos gestionados; estas opciones le permiten limitar el acceso administrativo exclusivamente a los dispositivos y áreas de la interfaz de gestión que necesita cada administrador para realizar su trabajo. De forma determinada, todos los servidores de Panorama vienen preconfigurados con una cuenta administrativa predeterminada (admin), que proporcionan acceso completo de lectura-escritura (también conocido como acceso de superusuario). Es recomendable que cree una cuenta administrativa diferente para cada persona que necesite acceder a las funciones de administración o informes de Panorama. Esto mejora la protección frente a la configuración no autorizada (o modificación) y permite el registro de acciones de cada uno de los administradores.

También puede definir un perfil de autenticación que determine cómo se comprueban las credenciales de acceso del usuario para todos los usuarios administrativos. Para aplicar un acceso administrativo más detallado, utilice los dominios de acceso para restringir el acceso administrativo a un dispositivo, grupo de dispositivos o plantilla concretos.

Funciones administrativas

La forma en la que configura las cuentas de administrador depende de los requisitos de seguridad de la organización, si tiene servicios de autenticación existentes con los que se quiere integrar y cuántas funciones administrativas distintas se necesitan. Una *función* define el tipo de acceso al sistema que tiene el administrador asociado. Hay dos tipos de funciones:

- **Funciones dinámicas**: funciones integradas que proporcionan acceso a Panorama y a los dispositivos gestionados: superusuario (acceso completo), superusuario (solo lectura) y administrador de Panorama.

  El administrador de Panorama no puede realizar las siguientes acciones:

  – Crear, modificar o eliminar administradores

  – Crear, modificar o eliminar funciones administrativas o dominios de acceso

  – Exportar, validar, invertir, guardar, cargar o importar la configuración de la pestaña **Dispositivo > Configuración**

  – Configurar la funcionalidad **Exportación de configuración programada** en la pestaña **Panorama**.

  Con las funciones dinámicas, no necesitará actualizar las definiciones de función, ya que se añaden nuevas características cuando las funciones se actualizan automáticamente.

- **Perfiles de función de administrador**: le permiten crear sus propias definiciones de función para ofrecer un control de acceso más detallado a las diversas áreas funcionales de la interfaz web, CLI o API XML. Los dos perfiles de función de administrador disponibles son: Panorama y Grupo de dispositivos y Plantilla. Podría crear un perfil de función de administrador para su personal de operaciones que proporcione acceso a grupos de dispositivos o plantillas específicos y un perfil separado para los administradores de seguridad que proporcione acceso a la definición de política de seguridad, logs e informes en Panorama. Tenga en cuenta que con los perfiles de función de administrador deberá actualizar los perfiles para asignar privilegios de forma explícita para nuevos componentes/características que se añadan al producto. De forma predeterminada, el acceso a todos los nuevos componentes y características está deshabilitado.

Consulte Configuración del acceso administrativo para crear funciones administrativas.

Perfiles y secuencias de autenticación

Entre otros usos, un perfil de autenticación define cómo se autentica a un usuario administrativo en Panorama al iniciar sesión. Si crea una cuenta de usuario local en Panorama, puede autenticar al usuario en la base de datos local o usar un servidor externo RADIUS, LDAP o Kerberos para la autenticación. Si no desea crear una cuenta de usuario local y quiere gestionar tanto la administración como la autenticación de la cuenta usando un mecanismo de autenticación externo, debe usar RADIUS. Para obtener una visión general de alto nivel del proceso, consulte Uso de los atributos específicos de proveedor (VSA) de RADIUS.

Para autenticar en varias fuentes de autenticación (local, RADIUS, LDAP o Kerberos), defina una secuencia de autenticación. Una secuencia de autenticación es un orden clasificado de perfiles de autenticación con los que se hace concordar a un usuario administrativo. Panorama siempre probará primero en la base de datos local y, a continuación, con cada perfil de la secuencia hasta identificar al usuario. Solo se impide el acceso del usuario a Panorama si falla la autenticación con todos los perfiles definidos en la secuencia de autenticación.

Para crear perfiles y secuencias de autenticación, consulte Creación de un perfil de autenticación y Definición de una secuencia de autenticación.

Dominios de acceso

Un dominio de acceso define las características y permisos correspondientes a un usuario administrativo, lo que permite el control detallado sobre la capacidad del usuario administrativo de cambiar el contexto y acceder a las características de la interfaz del usuario de los cortafuegos gestionados. Los dominios de acceso también pueden limitar el acceso a un subgrupo de grupos de dispositivos o plantillas creados en Panorama y, por lo tanto, restringir la capacidad del usuario para configurar y gestionar dispositivos.

El dominio de acceso está vinculado a atributos específicos del proveedor (VSA) RADIUS y únicamente se admite si se utiliza un servidor RADIUS para la autenticación del administrador. Si no se utiliza RADIUS, los ajustes de dominio de acceso se ignorarán. Para obtener información sobre cómo definir un dominio de acceso, consulte Definición de los dominios de acceso.

Autenticación administrativa

Hay cuatro formas de autenticar a usuarios administrativos:

- **Cuenta de administrador local con autenticación local**: tanto las credenciales de la cuenta de administrador como los mecanismos de autenticación son locales para el cortafuegos. Para añadir un nivel de protección adicional a la cuenta del administrador local, cree un perfil de contraseña que defina un período de validez para las contraseñas o establezca ajustes de complejidad de la contraseña para todo el dispositivo. Para obtener más información, consulte Creación de una cuenta administrativa.
- **Cuenta de administrador local con autenticación basada en certificado o clave**: con esta opción, las cuentas de administrador son locales en el cortafuegos, pero la autenticación se basa en claves SSH (para acceso a CLI) o certificados de cliente/tarjetas de acceso común (para la interfaz web). Para obtener más información sobre cómo configurar este tipo de acceso administrativo, consulte Activación de la autenticación basada en certificado para la interfaz web y Activación de la autenticación basada en claves de SSH para la interfaz de la línea de comandos.

- **Cuenta de administrador local con autenticación externa**: las cuentas de administrador se gestionan en el cortafuegos local, pero las funciones de autenticación se derivan a un servicio LDAP, Kerberos o RADIUS existente. Para configurar este tipo de cuenta, antes debe crear un perfil de autenticación que defina el modo de acceso al servicio de autenticación externa y después crear una cuenta para cada administrador que haga referencia al perfil. Si desea más información, consulte "Configuración de perfiles de autenticación" en el capítulo 3 de la *Guía del administrador de Palo Alto Networks*.

▲ **Cuenta y autenticación de administrador externas**: la administración y la autenticación de la cuenta las gestiona un servidor RADIUS externo. Para utilizar esta opción, debe definir atributos específicos de proveedor (VSA) en el servidor RADIUS que se asignen a la función de administrador. Para obtener una visión general de alto nivel del proceso, consulte Uso de los atributos específicos de proveedor (VSA) de RADIUS. Para obtener detalles sobre cómo configurar este tipo de acceso administrativo, consulte el artículo Radius Vendor Specific Attributes (VSA) (Atributos específicos de proveedor [VSA] en Radius.

Implementaciones recomendadas de Panorama

La implementación de Panorama consta del servidor de gestión de Panorama con una interfaz basada en navegador, los recopiladores de logs (opcionales) y los cortafuegos de Palo Alto Networks que se deben gestionar. Las implementaciones recomendadas de Panorama son:

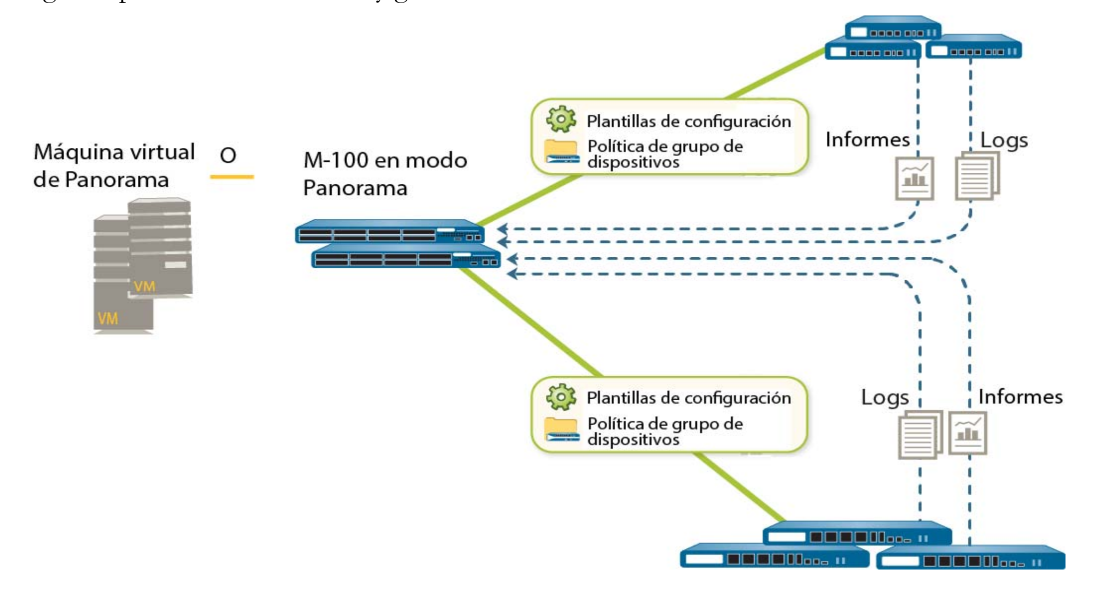
▲ Panorama para gestión centralizada y creación de informes

▲ Panorama en una arquitectura de recopilación de logs distribuida

Panorama para gestión centralizada y creación de informes

En el siguiente diagrama se explica cómo el dispositivo virtual de Panorama o el dispositivo M-100 se pueden implementar en una configuración redundante para ofrecer las siguientes ventajas:

- Gestión centralizada: política centralizada y gestión de dispositivos que permiten una implementación rápida y la gestión de hasta mil cortafuegos.
- Visibilidad: creación centralizada de logs y de informes para analizar e informar sobre el tráfico generado por el usuario y las posibles amenazas.
- Control de acceso basado en función: niveles adecuados de control administrativo a nivel de dispositivo y a nivel global para la administración y gestión.



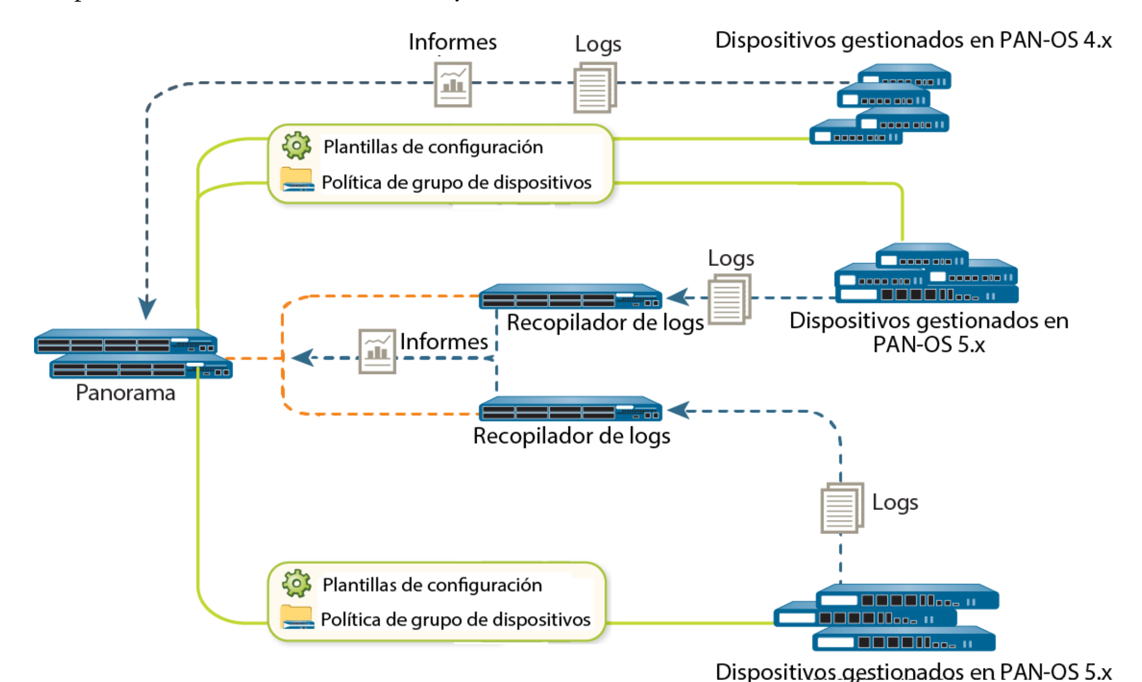
Panorama en una arquitectura de recopilación de logs distribuida

Panorama basado en hardware (dispositivo M-100) se puede implementar como un servidor de gestión de Panorama que realiza las funciones de gestión y de recopilación de logs o como un recopilador de logs especializado que proporciona una solución de recopilación de logs integral para los cortafuegos de la red. El uso del dispositivo M-100 como recopilador de logs permite un entorno más sólido donde el proceso de recopilación de logs se deriva a un dispositivo especializado. Mediante el uso de un dispositivo especializado en una arquitectura de recopilación de logs distribuida (DLC) se consigue redundancia, capacidad de ampliación mejorada y capacidad para un almacenamiento de logs de más duración.

En una arquitectura DLC, el servidor de gestión de Panorama (dispositivo virtual Panorama o M-100 en modo Panorama) gestiona los cortafuegos y los recopiladores de logs. Usando Panorama, los cortafuegos se configuran para enviar logs a uno o varios recopiladores de logs, Panorama se puede utilizar entonces para consultar los recopiladores de logs y proporcionar una vista agregada de tráfico de red. En una configuración DLC, se puede acceder a los logs almacenados en los recopiladores de logs desde los peers primario y secundario de Panorama en un clúster en alta disponibilidad (HA).

En la siguiente topología, los peers de Panorama en modo de alta disponibilidad gestionan la implementación y la configuración de cortafuegos que ejecutan PAN-OS 4.x y 5.x. Esta solución ofrece las siguientes ventajas:

- Permite un rendimiento mejorado en las funciones de gestión de Panorama
- Proporciona un almacenamiento de logs de alto volumen en un dispositivo de hardware especializado
- Proporciona escalabilidad horizontal y redundancia con un almacenamiento en RAID 1



Planificación de su implementación

- Compruebe las versiones de PAN-OS de los cortafuegos que se van a gestionar. Para gestionar los cortafuegos, Panorama debe estar ejecutando la misma versión o la más reciente que los cortafuegos que gestionará. Por ejemplo, un dispositivo Panorama 4.0 no puede gestionar dispositivos que ejecutan PAN-OS 5.0.
- Planifique el uso de la misma base de datos de filtrado de URL (BrightCloud o PAN-DB) en todos los cortafuegos gestionados. Si algunos cortafuegos utilizan la base de datos BrightCloud y otros utilizan PAN-DB, Panorama solo gestionará las políticas de seguridad de gestión para una de las bases de datos de filtrado de URL. Las reglas de filtrado de URL para la otra base de datos se deben gestionar localmente en los cortafuegos que utilizan esa base de datos.
- Planifique utilizar Panorama en una configuración de alta disponibilidad; configúrelo como un clúster en alta disponibilidad activo/pasivo. Consulte Alta disponibilidad de Panorama.
- Estime la capacidad de almacenamiento del log para la red. Para establecer el tamaño de la capacidad de almacenamiento del log con respecto a sus necesidades de seguridad y cumplimiento, debe considerar una serie de factores como la topología de red, el número de cortafuegos que envían logs, el tipo de tráfico de log (por ejemplo, logs de URL y amenazas frente a logs de tráfico), la velocidad a la que se generan los logs y el número de días que desea almacenar los logs en Panorama. Para obtener detalles, consulte el artículo: Panorama Logging Suggestions (Sugerencias sobre logs de Panorama).
- Para obtener informes de alto contenido sobre la actividad de la red, planifique una solución de registro:
  - ¿Necesita reenviar logs a un servidor Syslog, además de a Panorama?
  - Si necesita una solución de almacenamiento a largo plazo, ¿cuenta con una solución de gestión de eventos e información de seguridad (SIEM), como Splunk o ArcSight, a la que necesite reenviar los logs?
  - ¿Necesita redundancia en la creación de logs? Con los dispositivos virtuales de Panorama en HA, cada peer puede registrar en su disco virtual. Los dispositivos gestionados pueden enviar logs a los dos peers de un clúster en HA. Esta opción proporciona redundancia en la creación de logs y es la mejor para admitir hasta 2 TB de capacidad de almacenamiento de logs.
  - ¿Registra en un NFS? Solo se ofrece compatibilidad con NFS en el dispositivo virtual de Panorama. Considere utilizar NFS si se necesita una capacidad de almacenamiento de logs superior a 2 TB. Si se utiliza NFS, observe que los dispositivos gestionados solo pueden enviar logs al peer primario de un par de HA y que solo se monta el Panorama activo-primario en el NFS, en el que además se puede escribir.
- Determine el método de gestión. ¿Planea utilizar Panorama para configurar y gestionar las políticas o administrar las actualizaciones de software, contenido y licencia de forma centralizada? ¿o para centralizar la creación de logs e informes en todos los dispositivos gestionados de la red?

  If you have already deployed and configured the Palo Alto Networks firewalls on your network, determine whether to transition the devices to centralized management. Este proceso necesita migrar toda la configuración y las políticas de los cortafuegos a Panorama, consulte Transición de un dispositivo a una gestión central.
- Determine qué privilegios de acceso administrativos, funciones y permisos se necesitan para permitir el acceso a los cortafuegos gestionados y a Panorama. Consulte Configuración del acceso administrativo.

- Planifique los grupos de dispositivos necesarios. Para hacerlo, determine si desea agrupar los dispositivos según la función del dispositivo, la política de seguridad, la ubicación geográfica o la segmentación de la red. Por ejemplo, agrupe los dispositivos por función (aquellos destinados a las necesidades organizacionales de los socios o grupos funcionales de I+D) o agrupe los dispositivos que realizan la misma función (como los dispositivos de cortafuegos, dispositivos de sucursales o de centros de datos). Consulte Grupos de dispositivos.

- Planifique una estrategia de capa para administrar las políticas. Piense cómo deben heredarse y evaluarse las políticas y cómo implementar mejor las reglas compartidas, reglas de dispositivo-grupo y reglas específicas de dispositivos para cumplir las necesidades de su red.
  - Para tener visibilidad y conseguir una gestión de política centralizada, considere utilizar Panorama para administrar políticas, incluso si desea crear excepciones específicas de los dispositivos en políticas compartidas/de grupo-dispositivo. Para aplicar una regla a un subconjunto de dispositivos de un grupo de dispositivos, puede *dirigir* las reglas a uno o varios dispositivos concretos; consulte Dirección de políticas a un subconjunto de dispositivos.
  - Piense si desea crear grupos de dispositivos más pequeños basados en las características compartidas o crear grupos de dispositivos más grandes para realizar las ampliaciones de forma más sencilla. Consulte Uso de Panorama para configurar dispositivos gestionados: ejemplo.

- Planifique la organización del dispositivo para adaptarse a la forma en la que los ajustes de configuración (que usan plantillas) se heredan y se aplican. Por ejemplo, piense en cómo se asigna dispositivos a las plantillas basadas en plataformas de hardware, proximidad geográfica y necesidades de configuración de red similares para zonas horarias, servidor DNS y ajustes de la interfaz. Consulte Uso de Panorama para configurar dispositivos gestionados: ejemplo.

Implementación Panorama: Lista de comprobación de descripción general de tareas

En la siguiente lista de tareas se resumen los pasos para empezar a utilizar Panorama:

Paso 1. (solo dispositivo M-100) Monte el dispositivo en bastidor. Consulte la Guía de referencia de hardware de M-100.

Paso 2 Realice la configuración inicial para habilitar el acceso de red a Panorama. Consulte Configuración del dispositivo virtual de Panorama o Configuración del dispositivo M-100.

Paso 3 Instalación de licencias.

Paso 4 Instalación de las actualizaciones de contenido y software de Panorama.

Paso 5 Adición de dispositivos gestionados

Paso 6 Creación de grupos de dispositivos y Creación de plantillas.

Paso 7 (Opcional) Habilite la recopilación de logs en un recopilador de logs especializado. Consulte Habilitación de logs.

Paso 8 Supervise la actividad de la red usando las herramientas de visibilidad y creación de informes en Panorama. Consulte Supervisión de la red con el ACC y Appscope y Generación de informes.

Paso 9 Configure Panorama con unos ajustes de alta disponibilidad. Consulte Alta disponibilidad de Panorama.

Para ver un ejemplo de uso sobre cómo empezar a utilizar Panorama para una gestión centralizada, consulte el flujo de trabajo en Uso de Panorama para configurar dispositivos gestionados: ejemplo.

2 Configuración de Panorama

Para la realización centralizada de informes y una gestión de políticas cohesiva en todos los cortafuegos de la red, Panorama se puede implementar como dispositivo virtual o de hardware (el dispositivo M-100).

En los siguientes temas se describe cómo configurar Panorama en la red:

- Configuración del dispositivo virtual de Panorama
- Configuración del dispositivo M-100
- Migración de un dispositivo virtual de Panorama a un dispositivo M-100
- Navegación en la interfaz de usuario de Panorama
- Configuración del acceso administrativo

Configuración del dispositivo virtual de Panorama

El dispositivo virtual de Panorama consolida las funciones de gestión y log de Panorama en único dispositivo virtual. Esta solución permite el uso de una infraestructura virtual de VMware existente para implementar con facilidad y administrar y supervisar de forma centralizada los cortafuegos de Palo Alto Networks en su red, según se describe en las siguientes secciones:

- Requisitos
- Instalación de Panorama en el servidor ESX(i)
- Realización de la configuración inicial
- Ampliación de la capacidad de almacenamiento del log en el dispositivo virtual de Panorama



El dispositivo virtual de Panorama no se puede utilizar como recopilador de logs dedicado. Solo un dispositivo M-100 en modo de recopilación de logs proporciona funciones de recopilación de logs dedicadas. Sin embargo, puede gestionar un recopilador de logs usando el dispositivo virtual de Panorama. Consulte Configuración del dispositivo M-100 para obtener información detallada.

Requisitos

Para configurar eficazmente un dispositivo virtual de Panorama, compruebe que el servidor cumple los siguientes requisitos antes de comenzar:

- **Minimum System Requirements**

For Panorama version 5.1 Panorama version 5.1 is a 64-bit kernel-based VM	**For Panorama version 5.0 or earlier** Panorama version 5.0 or earlier use a 32-bit kernel-based VM
• VMware ESX(i) 4.1 o posterior • CPU de cuatro núcleos (2 GHz); utilice 3 GHz si tiene 10 o más cortafuegos • 4 GB de RAM; se recomiendan 16 GB si tiene 10 o más cortafuegos • 40 GB de espacio en disco Adding more disk space does not increase the available log storage capacity on Panorama. To expand log capacity, you must add a virtual disk or set up access to an NFS datastore. See Ampliación de la capacidad de almacenamiento del log en el dispositivo virtual de Panorama. • A client computer with one of the following: VMware vSphere Client or VMware Infrastructure Client that is compatible with your ESX(i) server	• VMware ESX(i) 3.5 o posterior • 2GHz CPU; use Quad Core CPU for optimal performance with high logging rates • 2GB RAM; 4GB recommended if have 10 or more firewalls • 40GB de espacio en disco Adding more disk space does not increase the available log storage capacity on Panorama. To expand log capacity, you must add a virtual disk or set up access to an NFS datastore. See Ampliación de la capacidad de almacenamiento del log en el dispositivo virtual de Panorama. • A client computer with one of the following: VMware vSphere Client or VMware Infrastructure Client that is compatible with your ESX(i) server



Los conceptos y terminología sobre VMware no se incluyen en este documento. Esta guía supone conocimientos sobre el conjunto de productos VMware necesario para crear el dispositivo virtual.

- Registre el número de serie de Panorama en el sitio de asistencia técnica en https://support.paloaltonetworks.com; el número de serie se le envió por correo electrónico. Tras registrar el número de serie en el sitio web de asistencia técnica, podrá acceder a la página de descargas de software de Panorama.

Instalación de Panorama en el servidor ESX(i)

Utilice estas instrucciones para instalar un nuevo dispositivo virtual de Panorama. Si está actualizando su dispositivo virtual de Panorama existente, vaya a Instalación de las actualizaciones de contenido y software de Panorama.

CREACIÓN DE UN PANORAMA VIRTUAL		
Paso 1.	Download and extract the Panorama base image zip file to the server on which you will be installing Panorama. La instalación del dispositivo virtual utiliza un archivo de plantilla de formato abierto de virtualización (OVF), que se incluye en la imagen base.	1. Vaya a https://support.paloaltonetworks.com/ y descargue el archivo zip de la **imagen base de Panorama**. 2. Descomprima el archivo zip de la imagen base de Panorama y extraiga el archivo **panorama-esx.ovf**. Este archivo de plantilla .ovf es necesario para instalar Panorama.
Paso 2	Acceda al servidor ESX(i).	Inicie el cliente VMware vSphere y conecte al servidor VMware.

CREACIÓN DE UN PANORAMA VIRTUAL		
Paso 3	Instale Panorama. Empezando con Panorama 5.1, el dispositivo virtual de Panorama se instala como una máquina virtual de 64 bits.	1. Seleccione **Archivo > Implementar plantilla de OVF**. 2. **Examine** para seleccionar el archivo panorama-esx.ovf desde la imagen base de Panorama descomprimida recientemente y haga clic en **Siguiente**. 3. Confirme que el nombre y la descripción del producto coinciden con la versión descargada y haga clic en **Siguiente**. 4. Introduzca un nombre descriptivo para el dispositivo virtual de Panorama y haga clic en **Siguiente**. 5. Seleccione una **ubicación del almacén de datos** en la que instalar la imagen de Panorama y haga clic en **Siguiente**. Adding additional disk space does not increase the available log storage capacity on Panorama. To expand log capacity, you must add a virtual disk or set up access to an NFS datastore. See Ampliación de la capacidad de almacenamiento del log en el dispositivo virtual de Panorama. 6. Seleccione **Thick Provision Lazy Zeroed (Suministro estándar diferido a cero)** como el formato de disco y haga clic en **Siguiente**. 7. Especifique las redes del inventario que se deben utilizar para el dispositivo virtual de Panorama. 8. Confirme las opciones seleccionadas y, a continuación, haga clic en **Finalizar** para comenzar el proceso de instalación.
		9. Cuando finalice la instalación, seleccione el dispositivo virtual de Panorama y haga clic en **Editar configuración...** para definir los siguientes ajustes: a. Verify that you have allocated the appropriate amount of memory. – Panorama 5.1: at least 4GB – Panorama 5.0 or earlier: 2 to 4GB b. Select the appropriate guest operating system. – Panorama 5.1: **Linux** as your **Guest Operating System** and **Version** as **Other Linux (64-bit)**. – Panorama 5.0 or earlier: **Linux** as your **Guest Operating System** and **Version** as **Other Linux (32-bit)** c. Choose the SCSI controller. – Panorama 5.1: **SCSI controller** is **LSI Logic Parallel** – Panorama 5.0 or earlier: **SCSI controller** is **Bus Logic Parallel**
Paso 4	Active el dispositivo virtual de Panorama.	Haga clic en el botón **Activar**. Cuando se reinicie el dispositivo virtual de Panorama, el proceso de instalación habrá finalizado.

Continúe con la Realización de la configuración inicial.

Realización de la configuración inicial

Utilice la consola del dispositivo virtual de Panorama en el servidor ESX(i) para configurar el acceso de red al dispositivo virtual de Panorama. Para completar la configuración inicial, en primer lugar debe configurar la interfaz de administración y, a continuación, acceder a la interfaz web de Panorama para añadir el número de serie para el dispositivo virtual y definir la zona horaria para el dispositivo virtual de Panorama. Para unificar informes, considere el uso de GMT o UTC como zona horaria uniforme para todos los dispositivos gestionados y Panorama.

CONFIGURACIÓN DE LA INTERFAZ DE GESTIÓN		
Paso 1.	Obtenga la información necesaria de su administrador de red.	• Dirección IP para el puerto MGT • Máscara de red • Puerta de enlace predeterminada • Dirección IP de servidor DNS
Paso 2	Acceda a la consola del dispositivo virtual de Panorama.	1. Seleccione la pestaña **Consola** del servidor ESX(i) para el Panorama virtual. Pulse Intro para acceder a la pantalla de inicio de sesión. 2. Introduzca el nombre de usuario/contraseña predeterminados (admin/admin) para iniciar sesión. 3. Introduzca **`configurar`** para pasar al modo de configuración.
Paso 3	Defina la configuración de acceso a la red para la interfaz de gestión. La interfaz de gestión se utiliza para el tráfico de gestión, la sincronización de la conectividad de HA, la recopilación de logs y la comunicación con los dispositivos del recopilador de logs.	Introduzca el siguiente comando: **`set deviceconfig system ip-address`** <*Panorama-IP*> **`netmask`** <*máscara de red*> **`default-gateway`** <*puerta de enlace-IP*> **`dns-setting servers primary`** <*DNS-IP*> donde <*Panorama-IP*> es la dirección IP que desea asignar la interfaz de gestión de Panorama, <*máscara de red*> es la máscara de subred, <*puerta de enlace-IP*> es la dirección IP de la puerta de enlace de red y <*DNS-IP*> es la dirección IP del servidor DNS.
Paso 4	Confirme los cambios y salga del modo de configuración.	Introduzca **`commit.`** Introduzca **`exit`**.
Paso 5	Verifique el acceso a la red para los servicios externos requeridos para la gestión del cortafuegos, como el servidor de actualizaciones de Palo Alto Networks:	Para verificar que Panorama tiene acceso de red externa, utilice la utilidad ping utility. Compruebe la conectividad a la puerta de enlace predeterminada, servidor DNS y el servidor de actualización de Palo Alto Networks como se muestra en el siguiente ejemplo: `admin@Panorama-Corp> ping host updates.paloaltonetworks.com` `Haciendo ping a updates.paloaltonetworks.com (67.192.236.252) con 56(84) bytes de datos.` `64 bytes desde 67.192.236.252: icmp_seq=1 ttl=243 tiempo=40.5 ms` `64 bytes desde 67.192.236.252: icmp_seq=1 ttl=243 tiempo=53.6 ms` `64 bytes desde 67.192.236.252: icmp_seq=1 ttl=243 tiempo=79.5 ms` **Nota** Cuando haya comprobado la conectividad, pulse Ctrl+C para detener los pings.

CÓMO AÑADIR UN NÚMERO DE SERIE Y ZONA HORARIA		
Paso 1.	Inicie sesión en la interfaz web de Panorama.	Si usa una conexión segura (https) desde un navegador web, inicie sesión usando la nueva dirección IP y la contraseña que asignó a la interfaz de gestión (https://<*dirección IP*>).
Paso 2	(Opcional) Modifique la configuración de la interfaz de gestión.	1. Seleccione **Panorama > Configuración > Gestión** y, a continuación, haga clic en el icono Editar de la sección Configuración de interfaz de gestión de la pantalla. 2. Seleccione los servicios de gestión que permitirá en la interfaz. Por ejemplo, para habilitar el acceso SSH, seleccione **SSH**. Es una práctica recomendada asegurarse de que ni Telnet ni HTTP estén seleccionados, ya que estos servicios usan texto plano, sin cifrar, y no son tan seguros como los otros servicios. 3. Haga clic en **ACEPTAR**. Haga clic en **Compilar** y seleccione Panorama como **Tipo**; a continuación, haga clic en **ACEPTAR**.
Paso 3	Añada el número de serie de Panorama. El número de serie se le envió en el correo electrónico de procesamiento del pedido.	1. Seleccione **Panorama > Configuración > Gestión** y haga clic en el icono Editar de la sección Configuración general de la pantalla. 2. Introduzca el **número de serie**.
Paso 4	Configure la zona horaria y la configuración general del cortafuegos.	1. Seleccione **Panorama > Configuración > Gestión** y haga clic en el icono Editar de la sección Configuración general de la pantalla. 2. Alinee el reloj de Panorama y de los cortafuegos gestionados para que utilicen la misma zona horaria, por ejemplo GMT o UTC. Las marcas de tiempo se registran cuando se reciben los logs en Panorama y cuando se generaron en los cortafuegos. La alineación de las zonas horarias en Panorama y en los dispositivos gestionados garantiza que las marcas de tiempo estén sincronizadas y que el proceso de consulta de los logs y de generación de informes en Panorama sea armónico. 3. Introduzca un **nombre de host** para el servidor y el nombre de **dominio** de red. El nombre de dominio tan solo es una etiqueta, no se usará para unirse al dominio. 4. Introduzca la **Latitud** y **Longitud** para permitir la colocación precisa del servidor en el mapamundi. 5. Haga clic en **ACEPTAR**.
Paso 5	Cambie la contraseña de administrador predeterminada. **Nota** Para garantizar la seguridad de la interfaz de gestión, puede aplicar la **complejidad de contraseña mínima** y definir un intervalo en el cual deben cambiar sus contraseñas los administradores.	1. Haga clic en el enlace del **administrador** en la parte inferior izquierda de la consola de gestión. Aparece un cuadro de diálogo para cambiar la contraseña del administrador. 2. Introduzca la antigua y la nueva contraseña en los campos correspondientes y guarde la nueva contraseña en un lugar seguro. 3. Haga clic en **ACEPTAR**.
Paso 6	Guarde sus cambios de configuración.	Haga clic en **Compilar** y seleccione Panorama como **Tipo**; a continuación, haga clic en **ACEPTAR**.

Ampliación de la capacidad de almacenamiento del log en el dispositivo virtual de Panorama

De forma predeterminada, el dispositivo virtual de Panorama se configura con una única partición de disco para todos los datos; se asignan unos 10 GB de este espacio para el almacenamiento de logs. Consulte el artículo Panorama Logging Suggestions (Sugerencias sobre logs de Panorama) para estimar la capacidad de almacenamiento de logs para sus requisitos y, a continuación, utilice una de las siguientes opciones para ampliar la capacidad de almacenamiento de los logs en el dispositivo virtual de Panorama:

- Cómo añadir un disco virtual en el servidor ESX(i) para ampliar el almacenamiento hasta un máximo de 2 TB.
- Configuración del acceso a un almacén de datos de NFS. Utilice esta opción si se necesita una capacidad de almacenamiento de logs superior a 2 TB.

Cómo añadir un disco virtual

El dispositivo virtual de Panorama se instala de forma predeterminada con un disco virtual con un tamaño de 34 GB, de los cuales 10,89 GB se destinan a logs. Para permitir un almacenamiento superior a 10 GB aprox., utilice el siguiente procedimiento para crear un nuevo disco virtual que admita hasta 2 TB de capacidad de almacenamiento.



El dispositivo virtual de Panorama solo puede utilizar un disco virtual. Cuando se configura para utilizar un disco virtual, el disco virtual no utiliza el almacenamiento interno de 10 GB para los logs. Por lo tanto, si pierde conectividad con el disco virtual, los logs se podrían perder durante el intervalo de fallo.

Para permitir la redundancia, utilice el disco virtual en una configuración de RAID. RAID 10 ofrece el mejor rendimiento de escritura para aplicaciones con características de registro elevado.

CÓMO AÑADIR UN DISCO VIRTUAL	
Paso 1. Desactive el dispositivo virtual de Panorama.	
Paso 2 En el servidor ESX(i), añada el disco virtual al dispositivo virtual de Panorama.	1. Seleccione el dispositivo virtual de Panorama en el servidor ESX(i). 2. Haga clic en **Editar configuración**. 3. Haga clic en **Añadir** para iniciar el asistente de adición de hardware y seleccione las siguientes opciones cuando se le solicite: a. Seleccione **Disco duro** para el tipo de hardware. b. Seleccione **Create a new virtual disk (Crear un nuevo disco virtual)**. c. Seleccione **SCSI** como el tipo de disco virtual. d. Seleccione el formato de disco **Thick Provisioning (Suministro estándar)**. e. En el campo de ubicación, seleccione **Store with the virtual machine option (Almacenar con la máquina virtual)**. **Nota** El almacén de datos no tiene que residir en el servidor ESX(i). f. Verifique que la configuración es correcta y haga clic en **Finalizar** para salir del asistente. El nuevo disco se añadirá a la lista de dispositivos del dispositivo virtual.

CÓMO AÑADIR UN DISCO VIRTUAL (CONTINUACIÓN)		
Paso 3	Active el dispositivo virtual de Panorama.	Cuando se activa, el disco virtual se inicializa para su primer uso. El tiempo que tarda en completarse el proceso de inicialización varía según el tamaño del nuevo disco virtual. Cuando el disco virtual se inicializa y se prepara, todos los logs existentes en el almacenamiento interno se desplazan al nuevo disco virtual. Todas las nuevas entradas se escriben ahora en el disco virtual.
Paso 4	Compruebe el tamaño del disco virtual.	1. Seleccione **Panorama > Configuración > Management (Gestión)**. 2. En la sección Configuración de log e informes, compruebe que la capacidad de **almacenamiento de log** muestra con precisión la nueva capacidad del disco.

Configuración del acceso a un almacén de datos de NFS

El montaje de un dispositivo virtual de Panorama en un almacén de datos de NFS ofrece la posibilidad de escribir logs en una ubicación centralizada y la flexibilidad de ampliar la capacidad de almacenamiento de los logs por encima de los 2 TB. Antes de configurar un almacenamiento de datos de NFS en una configuración de alta disponibilidad de Panorama, consulte Consideraciones sobre el registro en HA.

MONTAJE DE UN ALMACÉN DE DATOS DE NFS		
Paso 1.	Configure el acceso al almacén de datos.	1. Seleccione **Panorama > Configuración > Operaciones**. 2. Haga clic en el enlace **Configuración de partición de almacenamiento** en la sección Varios. 3. Seleccione **NFS V3**. 4. Introduzca la dirección IP del **servidor** NFS. 5. Introduzca la ubicación/ruta para almacenar los archivos log en el campo **Directorio de log**. Por ejemplo, export/panorama. 6. Seleccione el protocolo **TCP** o **UDP** e introduzca el **puerto** para acceder al servidor NFS. **Nota** Para utilizar NFS en TCP, el servidor NFS debe ser compatible. Los puertos NFS más frecuentes son UDP/TCP 111 para RPC y UDP/TCP 2049 para NFS. 7. Para el rendimiento óptimo de NFS, en los campos **Tamaño de lectura** y **Tamaño de escritura**, especifique el tamaño máximo de los grupos de datos que el cliente y el servidor se transfieren de uno a otro. La definición del tamaño de lectura/escritura optimiza el volumen y la velocidad de transferencia de los datos entre Panorama y el almacén de datos de NFS. 8. Seleccione **Partición de logs de prueba** para comprobar que Panorama puede acceder a la dirección IP del servidor de NFS y a la ubicación del directorio especificada anteriormente. 9. (Opcional) Seleccione la opción **Copiar al configurar**. Este ajuste copia los logs existentes almacenados en Panorama en el volumen de NFS. Si dispone de muchos logs, puede que permitir la copia en la opción de configuración inicie la transferencia de un gran volumen de datos. 10. Haga clic en **Compilar** y seleccione **Panorama** en **Compilar tipo** para guardar los cambios.

MONTAJE DE UN ALMACÉN DE DATOS DE NFS (CONTINUACIÓN)		
Paso 2	Reinicie el dispositivo virtual de Panorama. Hasta que se reinicia, los logs se escriben en el disco de almacenamiento local en el dispositivo virtual de Panorama.	Para empezar a escribir logs en el almacén de datos de NFS, reinicie el Panorama virtual. 1. Seleccione **Panorama > Configuración > Operaciones**. 2. En la sección Operaciones de dispositivo, seleccione la opción para **reiniciar Panorama**.

Determinación de una tasa de log en el cortafuegos de Palo Alto Networks

Utilice estas instrucciones en diferentes momentos del día para aproximar la tasa de generación de logs normal y de pico en todos los cortafuegos. Para estimar con precisión la cantidad de almacenamiento necesario para los logs en la red, además de la tasa de logs del cortafuegos, debe considerar otros factores. Para obtener detalles, consulte el artículo Panorama Logging Suggestions (Sugerencias sobre logs de Panorama).

VISUALIZACIÓN DE LA TASA DE GENERACIÓN DE LOGS		
Paso 1.	Acceda a la CLI de todos los cortafuegos de Palo Alto Networks.	Consulte Inicio de sesión en la CLI; el proceso de acceder a la CLI en el cortafuegos es el mismo que en Panorama.
Paso 2	Consulte la tasa de generación de logs actual.	Introduzca el siguiente comando CLI para valorar la tasa de logs en el cortafuegos: **`debug log-receiver statistics`** `Logging statistics` `----------------------------- --------` `Log incoming rate:            246/sec` `Log written rate:             246/sec`

¿Cuál es el siguiente paso?

Ahora que ha finalizado la configuración inicial, continúe con las siguientes secciones para obtener más instrucciones de configuración:

- Instalación de licencias
- Instalación de las actualizaciones de contenido y software de Panorama
- Navegación en la interfaz de usuario de Panorama
- Configuración del acceso administrativo
- Gestión de sus cortafuegos

Configuración del dispositivo M-100

El dispositivo de gestión M-100 es una plataforma de hardware de alto rendimiento que se puede implementar de dos formas:

- **Modo Panorama**: El dispositivo realiza tanto la función de gestión central como la de recopilación de logs. Es el modo predeterminado.
- **Modo de recopilación de logs**: El dispositivo actúa como recopilador de logs dedicado, que puede gestionarse ya sea mediante un dispositivo M-100 en modo Panorama o mediante un dispositivo virtual de Panorama. Si se reenvían grandes volúmenes de datos de logs desde varios cortafuegos, el dispositivo M-100 en el modo de recopilación de logs proporciona una escala y un rendimiento aumentados. Cuando se implementa en modo de recopilación de logs, el dispositivo no tiene una interfaz web, sino que el acceso administrativo solo es a través de la CLI.

Utilice el siguiente flujo de trabajo para configurar el dispositivo M-100:

Dispositivo M-100 en modo Panorama	Dispositivo M-100 en modo de recopilación de logs
Paso 1. Monte en rack el dispositivo M-100. Consulte la Guía de referencia de hardware de M-100 para obtener instrucciones.	Paso 1. Monte en rack el dispositivo M-100. Consulte la Guía de referencia de hardware de M-100 para obtener instrucciones.
Paso 2 Realización de la configuración inicial	Paso 2 Realización de la configuración inicial
Paso 3 Activación/recuperación de licencias	Paso 3 Activación/recuperación de licencias
Paso 4 Instalación de las actualizaciones de contenido y software de Panorama	Paso 4 Instalación de las actualizaciones de contenido y software de Panorama
Paso 5 (Opcional) Aumento de la capacidad de almacenamiento en el dispositivo M-100	Paso 5 (Opcional) Aumento de la capacidad de almacenamiento en el dispositivo M-100
Paso 6 Configuración del acceso administrativo	Paso 6 Configuración del dispositivo M-100 en modo de recopilación de logs
Paso 7 Gestión de sus cortafuegos	Paso 7 Habilitación de logs
Paso 8 Habilitación de logs	

Realización de la configuración inicial

De forma predeterminada, Panorama tiene una dirección IP de 192.168.1.1 y el nombre de usuario/contraseña es admin/admin. Por motivos de seguridad, debe cambiar estos ajustes antes de continuar con otras tareas de configuración. Debe realizar estas tareas de configuración inicial desde la interfaz de gestión o usando una conexión del puerto de serie directa al puerto de la consola del dispositivo M-100.

CONFIGURACIÓN DE LA INTERFAZ DE GESTIÓN		
Paso 1.	Obtenga la información necesaria de su administrador de red.	• Dirección IP para el puerto MGT • Máscara de red • Puerta de enlace predeterminada • Dirección de servidor DNS
Paso 2	Conecte su ordenador al dispositivo M-100.	Puede conectarse al dispositivo M-100 de uno de estos modos: • Conecte un cable serie desde un ordenador al puerto de la consola del dispositivo M-100 y conecte usando un software de emulación de terminal (9600-8-N-1). • Conecte un cable Ethernet RJ-45 desde un ordenador hasta el puerto de gestión del dispositivo M-100. Use un navegador para ir a **https://192.168.1.1.** Tenga en cuenta que tal vez deba cambiar la dirección IP de su ordenador a una dirección de la red 192.168.1.0, como 192.168.1.2, para acceder a esta URL.
Paso 3	Cuando se le indique, inicie sesión en el dispositivo.	Inicie sesión usando el nombre de usuario y contraseña predeterminados (admin/admin). El dispositivo comenzará a inicializarse.
Paso 4	Defina la configuración de acceso a la red para la interfaz de gestión. La interfaz de gestión se utiliza para el tráfico de gestión, la sincronización de la conectividad de HA, la recopilación de logs y la comunicación con los dispositivos del recopilador de logs.	1. Seleccione **Panorama > Configuración** y, a continuación, haga clic en el icono Editar de la sección Configuración de interfaz de gestión de la pantalla. 2. Introduzca la **dirección IP**, **máscara de red** y **puerta de enlace predeterminada**. 3. (Opcional) Seleccione los servicios de gestión que permitirá en la interfaz. Por ejemplo, habilite SSH. Es una práctica recomendada asegurarse de que ni Telnet ni HTTP estén seleccionados, ya que estos servicios usan texto plano, sin cifrar, y no son tan seguros como los otros servicios. 4. Haga clic en **ACEPTAR**. Haga clic en **Compilar** y seleccione Panorama como **Compilar Tipo** y, a continuación, haga clic en **ACEPTAR**.

CONFIGURACIÓN DE LA INTERFAZ DE GESTIÓN (CONTINUACIÓN)		
Paso 5	Establezca el nombre de host, la zona horaria y la configuración general.	1. Seleccione **Panorama > Configuración > Gestión** y haga clic en el icono Editar de la sección Configuración general de la pantalla. 2. Alinee el reloj de Panorama y de los cortafuegos gestionados para que utilicen la misma **zona horaria**, por ejemplo GMT o UTC. Establecer la misma zona horaria en Panorama y en los dispositivos gestionados garantiza que las marcas de tiempo de los logs están sincronizadas. Las marcas de tiempo se registran cuando se reciben los logs en Panorama y cuando se generaron en los cortafuegos. La alineación de las zonas horarias en Panorama y en los dispositivos gestionados garantiza que las marcas de tiempo estén sincronizadas y que el proceso de consulta de los logs y de generación de informes en Panorama sea armónico. 3. Introduzca un nombre de host para el servidor. Este nombre de host se utilizará como el nombre/etiqueta que se mostrará para el dispositivo. Por ejemplo, este es el nombre que aparecerá en el mensaje de la CLI y el que se mostrará en el campo Nombre del recopilador cuando añada el dispositivo como recopilador gestionado en la pestaña **Panorama > Recopiladores gestionados**. 4. Introduzca el nombre de dominio de red. El nombre de dominio tan solo es una etiqueta, no se usará para unirse al dominio. 5. Introduzca la **latitud** y longitud para permitir la colocación precisa del servidor en el mapamundi. Son los valores de latitud y longitud que se utilizarán en **Appscope > Traffic Maps (Mapas de tráfico)** y **Appscope > Threat Maps (Mapas de amenazas)**. 6. Haga clic en **ACEPTAR**.
Paso 6	Cambie la contraseña de administrador predeterminada. **Nota** Para garantizar la seguridad de la interfaz de gestión, puede aplicar la **complejidad de contraseña mínima** y definir el intervalo en el cual deben cambiar sus contraseñas los administradores.	1. Haga clic en el enlace del **administrador** en la parte inferior izquierda de la consola de gestión. Aparece un cuadro de diálogo para cambiar la contraseña del administrador. 2. Introduzca la antigua y la nueva contraseña en los campos correspondientes y guarde la nueva contraseña en un lugar seguro. Haga clic en **ACEPTAR**. 3. Haga clic en **Compilar** y seleccione Panorama como **Compilar Tipo**.

CONFIGURACIÓN DE LA INTERFAZ DE GESTIÓN (CONTINUACIÓN)		
Paso 7	Verifique el acceso a la red para los servicios externos requeridos para la gestión del cortafuegos, como el servidor de actualizaciones de Palo Alto Networks.	Para verificar que Panorama tiene acceso de red externa, utilice la utilidad ping utility. Compruebe la conectividad a la puerta de enlace predeterminada, servidor DNS y el servidor de actualización de Palo Alto Networks como se muestra en el siguiente ejemplo: `admin@Panorama-Corp> ping host updates.paloaltonetworks.com` `Haciendo ping a updates.paloaltonetworks.com (67.192.236.252) con 56(84) bytes de datos.` `64 bytes desde 67.192.236.252: icmp_seq=1 ttl=243 tiempo=40.5 ms` `64 bytes desde 67.192.236.252: icmp_seq=1 ttl=243 tiempo=53.6 ms` `64 bytes desde 67.192.236.252: icmp_seq=1 ttl=243 tiempo=79.5 ms` **Nota** Cuando haya comprobado la conectividad, pulse Ctrl+C para detener los pings.

Continúe con Instalación de licencias y Instalación de las actualizaciones de contenido y software de Panorama, independientemente de si planea utilizar el dispositivo M-100 en el modo Panorama o de recopilación de logs.

Configuración del dispositivo M-100 en modo de recopilación de logs

El uso del dispositivo M-100 como recopilador de logs evita la tarea de procesar los logs en un dispositivo dedicado. Utilice las instrucciones de esta sección para convertir el dispositivo M-100 del modo Panorama al modo de recopilación de logs para implementarlo como recopilador de logs dedicado. Asegúrese de que el dispositivo de Panorama que gestionará los cortafuegos y el recopilador de logs ya se ha configurado.



En el modo de recopilación de logs, el dispositivo M-100 no es compatible con la interfaz web para las tareas de configuración; solo se admite el acceso SSH. Por lo tanto, antes de cambiar el modo en el dispositivo M-100, conviene la Realización de la configuración inicial y la utilización de la interfaz web en el modo Panorama para la Activación/recuperación de licencias.

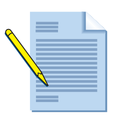
Para enviar registros a un dispositivo M-100 en el modo de recopilación de logs, los cortafuegos de Palo Alto Networks deben ejecutar PAN-OS v5.0 o versiones posteriores. Los cortafuegos de Palo Alto Networks que ejecutan versiones de PAN-OS anteriores a 5.0 solo pueden enviar logs a un dispositivo M-100 en el modo Panorama o en un dispositivo virtual de Panorama.

CAMBIO DEL MODO PANORAMA AL MODO DE RECOPILACIÓN DE LOGS		
Paso 1.	Acceda a la interfaz de línea de comandos (CLI) en el dispositivo M-100.	Conéctese al dispositivo M-100 de uno de estos modos: • Conecte un cable serie desde un ordenador hasta el puerto de consola del dispositivo M-100. A continuación, conéctese usando un software de emulación de terminal (9600-8-N-1). • Use un software de emulación de terminal como PuTTY para abrir una sesión SSH en la dirección IP asignada al dispositivo M-100 durante la configuración inicial.
Paso 2	Cuando se le indique, inicie sesión en el dispositivo.	Utilice la cuenta y la contraseña *admin* predeterminadas asignadas durante la configuración inicial.
Paso 3	Cambio del modo Panorama al modo de recopilación de logs.	1. Para cambiar al modo de recopilación de logs, introduzca el siguiente comando: **`request system logger-mode logger`** 2. Introduzca **`Yes`** para confirmar el cambio del modo de recopilación de logs. El dispositivo se reiniciará.
Paso 4	Compruebe que el dispositivo está en modo de recopilación de logs.	1. Vuelva a iniciar sesión en la CLI en el dispositivo M-100. 2. Introduzca el siguiente comando: **`show system info | match logger_mode`** La respuesta que aparece en pantalla es *`logger_mode: True`* Si el valor aparece como **`False`**, el dispositivo M-100 sigue en modo Panorama.
Paso 5	Especifique la dirección IP del dispositivo Panorama que gestiona este recopilador de logs.	Introduzca el siguiente comando en la CLI: **`configure`** **`set panorama-server`** *`<ip_address>`* **`commit`**

Ahora que ha configurado correctamente el dispositivo M-100, para obtener más información sobre cómo asignar un recopilador de logs a un cortafuegos, designar grupos de recopiladores y gestionar el recopilador de logs usando Panorama, consulte Habilitación de logs.

Aumento de la capacidad de almacenamiento en el dispositivo M-100

El dispositivo M-100 se suministra con dos discos en una configuración RAID1. Todos los dispositivos M-100 permiten añadir hasta tres pares de discos adicionales en RAID1, cada uno con una capacidad de almacenamiento de 1 TB, para alcanzar una capacidad máxima de almacenamiento de RAID de 4 TB.



Si se añaden pares de discos a un dispositivo M-100 que ya se ha implementado, no hay necesidad de que el dispositivo esté fuera de línea para ampliar la capacidad de almacenamiento. Cuando los pares de discos adicionales estén disponibles, el dispositivo M-100 redistribuirá los logs entre los pares de discos disponibles. El proceso de redistribución de logs se produce en segundo plano y no tiene influencia en el tiempo de actividad o la disponibilidad del dispositivo M-100.

CONFIGURACIÓN DE LOS DISCOS EN UN PAR RAID		
Paso 1.	Instale los nuevos discos en las bahías de unidades adecuadas.	Asegúrese de añadir unidades secuencialmente en la siguiente ranura de bahía de discos abierta para el par de discos. Por ejemplo, añada B1/B2 antes de C1/C2. Para obtener más información sobre cómo añadir unidades físicas, consulte Guía de referencia de hardware de M-100.
Paso 2	Acceda a la interfaz de línea de comandos (CLI) en el dispositivo M-100.	Puede conectarse al dispositivo M-100 de uno de estos modos: • Conecte un cable serie desde su ordenador al puerto de la consola y conecte el dispositivo M-100 usando el software de emulación de terminal (9600-8-N-1). • Use un software de emulación de terminal como PuTTY para abrir una sesión SSH en la dirección IP asignada al dispositivo M-100.
Paso 3	Cuando se le indique, inicie sesión en el dispositivo.	Utilice la cuenta y la contraseña *admin* predeterminadas asignadas.

<table>
<tr><th colspan="3">CONFIGURACIÓN DE LOS DISCOS EN UN PAR RAID (CONTINUACIÓN)</th></tr>
<tr><td>Paso 4</td><td>Configure todos los pares de discos adicionales en una configuración RAID.

Nota El tiempo necesario para reflejar los datos en la unidad puede variar entre algunos minutos a horas, dependiendo de la cantidad de datos almacenados en la unidad.</td><td>En este ejemplo se utilizan las unidades de las bahías de discos B1 y B2.
1. Introduzca los siguientes comandos y confirme la solicitud cuando se le indique:
<code>request system raid add B1</code>
<code>request system raid add B2</code>
2. Para supervisar el progreso de la configuración RAID, introduzca el siguiente comando:
<code>show system raid detail</code>
Cuando la configuración de RAID finalice, aparece la siguiente respuesta:<pre>
Disk Pair A   Available
   Status   clean
   Disk id A1   Present
       model   : ST91000640NS
       size   : 953869 MB
       status   : active sync
   Disk id A2   Present
       model   : ST91000640NS
       size   : 953869 MB
       status   : active sync
Disk Pair B   Available
   Status   clean
   Disk id B1   Present
       model   : ST91000640NS
       size   : 953869 MB
       status   : active sync
   Disk id B2   Present
       model   : ST91000640NS
       size   : 953869 MB
       status   : active sync
</pre></td></tr>
<tr><td>Paso 5</td><td>Haga que el par de discos esté disponible para la realización de logs.

Para habilitar los pares de discos para la realización de logs, este dispositivo se debe haber añadido como recopilador gestionado en Panorama. Si todavía no lo ha añadido, consulte Adición de un recopilador de logs a Panorama.</td><td>1. Acceda al servidor de gestión de Panorama que esté gestionando este recopilador de logs (si se trata de un dispositivo distinto).
2. En la pestaña Panorama > Recopiladores gestionados, seleccione el recopilador de logs y siga las instrucciones del Paso 6 en Adición de un recopilador de logs a Panorama.</td></tr>
<tr><td>Paso 6</td><td>Guarde sus cambios de configuración.</td><td>Haga clic en Confirmar. Seleccione Panorama como Compilar Tipo y haga clic en ACEPTAR.</td></tr>
</table>

Para obtener más instrucciones sobre cómo añadir un recopilador de logs como recopilador gestionado en Panorama, definir grupos de recopiladores, asignar un recopilador de logs a un cortafuegos, consulte Habilitación de logs.

Migración de un dispositivo virtual de Panorama a un dispositivo M-100

En un dispositivo virtual de Panorama que gestiona 10 o más dispositivos y que tiene una tasa de log de más 10.000 logs por segundo, la migración al dispositivo M-100 proporcionará una respuesta mejorada en la interfaz web y una ejecución de informes más rápida. El dispositivo M-100 también proporciona hasta 4 TB de almacenamiento RAID. Utilice las instrucciones de esta sección para migrar la configuración desde el dispositivo virtual de Panorama hasta un dispositivo M-100.

- ▲ Requisitos
- ▲ Consideraciones de planificación
- ▲ Realización de la migración
- ▲ Reanudación de la gestión de dispositivos

Requisitos

Para continuar con la migración de la suscripción actual, debe haber:

- Adquirido un dispositivo M-100
- Obtenido una actualización de migración y adquirido una nueva suscripción que incluya asistencia técnica para software y hardware.

  Para procesar la actualización de la migración debe haberse puesto en contacto con su representante de ventas con lo siguiente:

  – Número de serie de la versión de Panorama virtual que quiere actualizar

  – Términos de asistencia técnica para el dispositivo M-100 y código de autorización recibido al adquirir el dispositivo

  – Fecha en la que entrará en vigor la migración

    Palo Alto Networks aplicará automáticamente los códigos de autorización asociados al número de serie del dispositivo de gestión, revertirá la asistencia técnica de la versión de Panorama virtual existente y activará la asistencia técnica para el dispositivo M-100 en la fecha de entrada en vigor seleccionada.

    Desde la fecha de entrada en vigor, tendrá un límite de tiempo para completar el proceso de migración. Al final del periodo, el derecho a la asistencia técnica en el dispositivo virtual de Panorama se anulará y ya no recibirá actualizaciones de software o sobre amenazas. Consulte este artículo para obtener detalles sobre el proceso de migración de la licencia.

Consideraciones de planificación

- Planifique cómo completar esta migración en una ventana de mantenimiento. Aunque los cortafuegos pueden almacenar los logs en el búfer y reenviarlos a Panorama cuando la conexión se restablezca, completar la migración en una ventana de mantenimiento minimiza la pérdida de datos del log durante el tiempo de transición en el que el dispositivo virtual de Panorama queda fuera de línea y el dispositivo M-100 entra en línea.
- Piense si desea mantener el acceso al dispositivo virtual de Panorama después de completar la migración. Como el formato de log del dispositivo virtual de Panorama no es compatible con el del dispositivo M-100, los datos del log existentes no pueden migrar al dispositivo M-100. Por lo tanto, para acceder a logs antiguos, el dispositivo virtual de Panorama debe permanecer accesible.
- Decida si desea utilizar la misma dirección IP del dispositivo M-100 o asignar una nueva. Palo Alto Networks recomienda volver a utilizar la misma dirección IP de gestión para evitar la necesidad de reconfigurar los dispositivos gestionados para que indiquen una nueva dirección IP.



Si tiene requisitos de cumplimiento para los logs, planifique reconfigurar una nueva dirección IP en el dispositivo virtual de Panorama para mantener el acceso a los antiguos logs para generar informes.

- Mantenga una *nueva* dirección IP, disponible para utilizar al configurar la conectividad en el dispositivo M-100 durante la configuración inicial. Si ha decidido transferir la dirección IP asignada al dispositivo virtual de Panorama, esta nueva dirección IP se utilizará temporalmente. Cuando restaure el archivo de configuración desde el dispositivo virtual de Panorama en el dispositivo M-100, se sobrescribirá esta *nueva* dirección IP.

Realización de la migración

Para migrar la configuración del dispositivo virtual de Panorama al dispositivo M-100, complete las siguientes tareas:

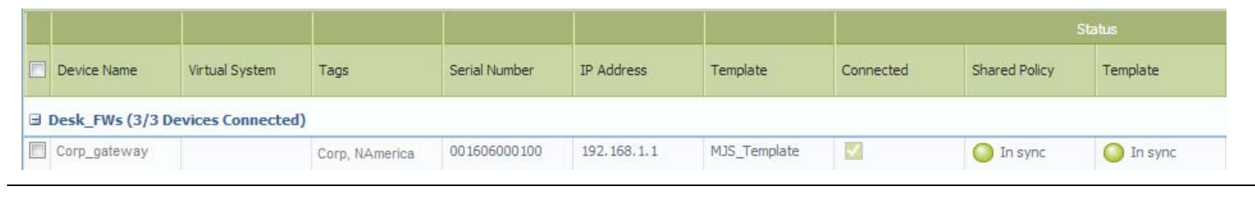
MIGRACIÓN DESDE EL DISPOSITIVO VIRTUAL DE PANORAMA	
Paso 1. Complete estas tareas en el dispositivo virtual de Panorama.	
1. Actualice a la última versión de Panorama.	Consulte Instalación de las actualizaciones de contenido y software de Panorama.
2. Exporte la configuración que se está ejecutando en el dispositivo Panorama virtual.	1. En la pestaña **Panorama > Configuración > Operaciones**, en la sección Gestión de configuración, seleccione **Exportar copia de configuración con nombre Panorama**. 2. Seleccione la configuración activa (running-config.xml) y haga clic en **ACEPTAR**. El archivo se descarga y se guarda en la máquina local. 3. Cambie el nombre del archivo.
3. Apague la VM o cambie la dirección IP.	Si planea volver a utilizar la dirección IP de la interfaz de gestión configurada en el dispositivo virtual de Panorama en el dispositivo M-100, puede apagar el dispositivo virtual o asignar una nueva dirección IP al puerto de gestión del dispositivo virtual. Para cambiar la dirección IP, en la pestaña **Panorama > Configuración**, edite la sección **Configuración de interfaz de gestión** e introduzca la nueva dirección IP.
Paso 2 Complete estas tareas en el dispositivo M-100.	
1. Configure el acceso de red.	Consulte Realización de la configuración inicial para obtener instrucciones. Considere asignar una nueva dirección IP *temporal* durante la configuración inicial del dispositivo M-100 y volver a utilizar la dirección IP asignada al dispositivo virtual de Panorama. La dirección IP temporal se sobrescribirá cuando importe la configuración más adelante en el proceso.
2. Instale la misma versión de Panorama que la que se ejecuta en el dispositivo virtual de Panorama.	Instale la misma versión de Panorama seleccionada en el Paso 1 anterior. Para obtener instrucciones sobre cómo realizar la actualización, consulte Instalación de las actualizaciones de contenido y software de Panorama.
3. Registre Panorama y recupere la licencia.	Consulte Instalación de licencias.

MIGRACIÓN DESDE EL DISPOSITIVO VIRTUAL DE PANORAMA (CONTINUACIÓN)	
4. Importe y cargue el archivo de configuración.	1. En la pestaña **Panorama > Configuración > Operaciones**, sección Gestión de configuración, seleccione **Importar configuración Panorama por nombre**. 2. **Examine** para seleccionar running-config.xml (o el archivo al que se le ha cambiado el nombre) y haga clic en **ACEPTAR**. 3. Seleccione el enlace **Cargar configuración con nombre Panorama** para cargar el archivo de configuración que acaba de importar. Cualquier error que se produzca al cargar el archivo de configuración aparecerá en pantalla. 4. Si hubiera errores, guárdelos en un archivo local. Revise y resuelva cualquier error para asegurarse de que todos los componentes de la configuración se han migrado.
5. Revise y modifique la configuración en Panorama.	1. Si no planea reutilizar la misma configuración de acceso a la red para la interfaz de gestión, modifique los valores: a. Seleccione **Panorama > Configuración** y, a continuación, haga clic en el icono Editar de la sección Configuración de interfaz de gestión de la pantalla. b. Introduzca la **dirección IP**, **máscara de red** y **puerta de enlace predeterminada**. c. Confirme que la lista de direcciones IP definidas en la lista Direcciones IP permitidas es precisa. 2. Para cambiar el nombre de host, edite la sección Configuración general de la pestaña **Panorama > Configuración**. 3. Confirme que la configuración del acceso administrativo (administradores, funciones y dominios de acceso) seleccionada en el dispositivo es precisa en la pestaña **Panorama > Administradores**, **Panorama > Funciones de administrador** y en la pestaña **Panorama > Dominios de acceso (Access Domains)**.
6. Vuelva a añadir el recopilador de logs predeterminado al dispositivo M-100.	Cuando se importa la configuración desde el dispositivo virtual de Panorama, el recopilador de logs predeterminado se elimina del dispositivo M-100. Para volver a añadir el recopilador de logs al dispositivo M-100, utilice las instrucciones de Adición de un recopilador de logs a Panorama.
7. Guarde todos los cambios realizados en Panorama.	Después de revisar los cambios de configuración, haga clic en **Compilar**. Seleccione Panorama como **Compilar Tipo** y haga clic en **ACEPTAR**.

Reanudación de la gestión de dispositivos

Para reanudar la gestión central, debe restaurar la conectividad de los dispositivos gestionados. Complete esta tarea en una ventana de mantenimiento para minimizar el tiempo de interrupción de la red.

VERIFICACIÓN DEL ESTADO DE LOS DISPOSITIVOS GESTIONADOS		
Paso 1.	Inicie sesión en Panorama.	Mediante una conexión segura (https) desde un navegador web, inicie sesión usando la dirección IP y la contraseña asignada durante la configuración inicial (https://<*dirección IP*>).
Paso 2	Sincronice la configuración de Panorama con la del dispositivo gestionado.	1. Seleccione **Panorama > Dispositivos gestionados** y compruebe que el estado **Conectado** de los dispositivos aparece con la marca ✓. El estado de las plantillas y grupos de dispositivos aparecerá como Out of sync . 2. Para sincronizar los grupos de dispositivos: a. Haga clic en **Compilar** y seleccione **Grupos de dispositivos** como **Compilar tipo**. b. Seleccione cada uno de los grupos de dispositivos y haga clic en **ACEPTAR**. 3. Para sincronizar las plantillas: a. Haga clic en **Compilar** y seleccione **Panorama** como **Compilar tipo**. b. Haga clic en **Compilar** y seleccione **Plantilla** como **Compilar tipo**.
Paso 3	Compruebe el estado de los dispositivos, plantillas y política compartida está **Conectado** y **In sync (Sincronizado)**.	



Instalación de licencias

Antes de empezar a utilizar Panorama para una gestión centralizada, realizar logs y crear informes debe registrar Panorama y recuperar las licencias.

Todas las instancias de Panorama necesitan licencias válidas que le permitan gestionar dispositivos y obtener asistencia técnica. La licencia de gestión de dispositivos activa el número máximo de dispositivos que Panorama puede gestionar. La licencia de asistencia técnica permite las actualizaciones de software de Panorama y las de contenido dinámico para las últimas firmas de amenazas y aplicaciones, entre otras, publicadas por Palo Alto Networks.

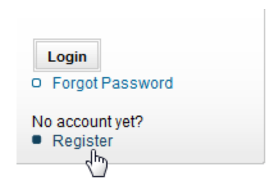
Para adquirir licencias, póngase en contacto con su ingeniero de sistemas de Palo Alto Networks o distribuidor. Después de obtener una licencia, desplácese hasta **Panorama > Licencias** para realizar la siguientes tareas dependiendo de cómo reciba las licencias:

- **Recuperar claves de licencia del servidor de licencias:** utilice esta opción si la licencia se ha activado en el portal de asistencia técnica.
- **Activar característica mediante código de autorización:** utilice el código de autorización para activar una licencia que no se ha activado anteriormente en el portal de asistencia técnica.
- **Carga manual de la clave de licencia:** utilice esta opción si Panorama no tiene conectividad con el servidor de actualización de Palo Alto Networks. En este caso, en primer lugar debe descargar un archivo de clave de licencia del sitio de asistencia técnica a través de un ordenador conectado a Internet y después cargarlo en Panorama.

Registro de Panorama

Para gestionar todos los activos adquiridos en Palo Alto Networks, debe crear una cuenta y registrar los números de serie con la cuenta.

REGISTRO CON PALO ALTO NETWORKS		
Paso 1.	Inicie sesión en la interfaz web de Panorama.	Si usa una conexión segura (https) desde un navegador web, inicie sesión usando la dirección IP y la contraseña que asignó durante la configuración inicial (https://<*dirección IP*>).
Paso 2	Busque el número de serie y cópielo en el portapapeles.	• El número de serie del dispositivo M-100 aparece en el **Panel**; encuentre el **Número de serie** en la sección Información general de la pantalla. • En el dispositivo virtual de Panorama, el número de serie venía incluido en el correo electrónico de procesamiento del pedido.
Paso 3	Vaya al sitio de asistencia de Palo Alto Networks.	En una ventana o pestaña nueva del navegador, vaya a https://support.paloaltonetworks.com.

REGISTRO CON PALO ALTO NETWORKS (CONTINUACIÓN)		
Paso 4	Registro de Panorama. El modo de registrarse dependerá de que tenga o no un inicio de sesión en el sitio de asistencia técnica.  	• Si es el primer dispositivo de Palo Alto Networks que registra y aún no tiene un inicio de sesión, haga clic en **Registrar** en el lado derecho de la página. Para registrarse, debe proporcionar su dirección de correo electrónico y el número de serie de Panorama (que puede pegar desde el portapapeles). Cuando se le solicite, establezca un nombre de usuario y una contraseña para acceder a la comunidad de asistencia técnica de Palo Alto Networks. • Si ya dispone de una cuenta de asistencia técnica, inicie sesión y haga clic en **Mis dispositivos**. Desplácese hasta la sección Registrar dispositivo, en la parte inferior de la pantalla, e introduzca el número de serie de Panorama (que puede pegar desde el portapapeles), su ciudad y su código postal, y haga clic en **Registrar dispositivo**.

Activación/recuperación de licencias

Todos los dispositivos de Panorama, el factor de forma virtual y el dispositivo basado en hardware, requieren una licencia válida.



Si ejecuta una licencia de evaluación en el dispositivo virtual de Panorama y desea aplicar una licencia de Panorama que ha adquirido:

1. Registre el número de serie de Panorama en el sitio de asistencia técnica de Palo Alto Networks. Consulte el Paso 4 de Registro de Panorama.
2. Seleccione **Panorama > Configuración > Gestión** y haga clic en el icono Editar de la sección Configuración general.
3. Introduzca el **número de serie** para el dispositivo virtual de Panorama y haga clic en **Compilar** para compilar los cambios en Panorama. La licencia se aplica automáticamente a Panorama.

ACTIVACIÓN DE LA LICENCIA		
Paso 1.	Encuentre los códigos de activación del producto/suscripción que ha adquirido.	Al realizar el pedido, debió recibir un mensaje de correo electrónico del servicio de atención al cliente de Palo Alto Networks con los códigos de autorización asociados a la compra. Si no encuentra este mensaje, póngase en contacto con atención al cliente para recibir sus códigos antes de continuar.

ACTIVACIÓN DE LA LICENCIA (CONTINUACIÓN)

Paso 2 Activación de la licencia.

El dispositivo M-100 requiere tanto la suscripción a la asistencia técnica como la licencia de gestión del dispositivo.

El dispositivo virtual de Panorama solo requiere la suscripción a la asistencia técnica. La función de gestión del dispositivo se habilita al añadir el número de serie.

Nota Si el puerto de gestión de Panorama no tiene acceso a Internet, descargue manualmente los archivos de licencia desde el sitio de asistencia técnica y cárguelos en Panorama usando la opción **Clave de licencia de carga manual**.

1. Para activar la suscripción a la asistencia técnica, seleccione **Panorama > Asistencia técnica**.
2. Seleccione **Activar característica mediante código de autorización**. Introduzca el **Código de autorización** y, a continuación, haga clic en **Aceptar**.
3. Compruebe que la suscripción se haya activado correctamente.

Support	
Phone	866-898-9087
Email	support@paloaltonetworks.com
ExpiryDate	October 01, 2015
Level	Premium
Description	24 x 7 phone support; advanced replacement hardware service
	Activate support using authorization code

4. (Sólo necesario para el dispositivo M-100) En la pestaña **Panorama > Licencias**, seleccione **Activar característica mediante código de autorización**.
5. Cuando se le solicite, introduzca **Código de autorización** para usar Panorama y haga clic en **ACEPTAR**.
6. Compruebe que la licencia se ha activado correctamente y que indica asistencia técnica para el número correcto de dispositivos. Por ejemplo:

Device Management License	
Date Issued	September 04, 2012
Date Expires	Never
Description	Device management license to manage up to 25 devices

Nota Para el dispositivo virtual de Panorama, puede ver la licencia de gestión de dispositivos solamente en el portal de asistencia técnica.

Paso 3 (No es necesario si ha completado el paso 2) Recupere las claves de licencia del servidor de licencias.

Utilice la opción **Recuperar claves de licencia del servidor de licencias** si ha activado las claves de licencia en el portal de asistencia técnica.

Seleccione **Panorama > Asistencia técnica** y seleccione **Recuperar claves de licencia del servidor de licencias**.

Instalación de las actualizaciones de contenido y software de Panorama

La suscripción a la asistencia técnica válida habilita la imagen de software y las notas de versión de Panorama. Es recomendable usar la actualización más reciente del software o la versión recomendada por su distribuidor o por el ingeniero de sistemas de Palo Alto Networks con el fin de aprovechar las correcciones y mejoras de seguridad más recientes.



Importante: Panorama versión 5.1 solo está disponible como sistema operativo de 64 bits. Antes de actualizar un dispositivo virtual de Panorama a la versión 5.1, asegúrese de que el host ESX(i) admite un sistema operativo de 64 bits y que cumple los requisitos mínimos del sistema para el sistema operativo de 64 bits. Consulte Requisitos para obtener más información.

Si se gestionan dispositivos con suscripciones adicionales, como Prevención de amenazas o WildFire, Panorama también necesita las actualizaciones de contenido para las bases de datos de aplicaciones y amenazas. La suscripción de asistencia le permite obtener estas actualizaciones. Se hace referencia a las bases de datos de aplicaciones y amenazas en las configuraciones de política, las cuales se utilizan cuando se generan informes; estas bases de datos se utilizan para hacer coincidir los identificadores registrados en los logs con la amenaza, URL o nombre de aplicación correspondientes. Por lo tanto, para evitar la falta de coincidencias, Palo Alto Networks recomienda que instale la misma versión de la base de datos de aplicaciones y amenazas en Panorama y en los dispositivos gestionados.

REALIZACIÓN DE LAS ACTUALIZACIONES DE VERSIÓN DE CONTENIDO Y PANORAMA		
Paso 1.	Inicie la interfaz web de Panorama y vaya a la página de actualizaciones dinámicas. Antes de actualizar el software, instale las últimas actualizaciones de contenido admitidas en esta versión.	1. Si usa una conexión segura (https) desde un navegador web, inicie sesión usando la dirección IP y la contraseña que asignó durante la configuración inicial (https://<*dirección IP*>). 2. Seleccione **Panorama > Actualizaciones dinámicas**.
Paso 2	Busque, descargue e instale la última actualización de base de datos de contenido. Instale las actualizaciones de aplicaciones y amenazas antes de instalar la actualización del antivirus.	1. Haga clic en **Comprobar ahora** para comprobar las actualizaciones más recientes. Si el valor de la columna Acción es **Descargar** significa que hay una actualización disponible. 2. Haga clic en **Descargar** para obtener la versión deseada. 3. Haga clic en el enlace **Instalar** de la columna Acción. Cuando se complete la instalación, aparecerá una marca de verificación en la columna Instalado actualmente.
Paso 3	Compruebe las actualizaciones de software.	1. Seleccione **Panorama > Software**. 2. Haga clic en **Comprobar ahora** para comprobar las actualizaciones más recientes. Si el valor de la columna **Acción** es **Descargar** significa que hay una actualización disponible.

REALIZACIÓN DE LAS ACTUALIZACIONES DE VERSIÓN DE CONTENIDO Y PANORAMA (CONTINUACIÓN)

Paso 4 Descargar la actualización.

Nota Si Panorama no tiene acceso a Internet desde el puerto de gestión, puede descargar la actualización de software desde el sitio de asistencia técnica de Palo Alto Networks. Después podrá **cargarla** manualmente en Panorama.

Encuentre la versión a la que desea actualizar y haga clic en **Descargar**. Cuando se complete la descarga, el valor en la columna Acción cambia a **Instalar**.

Version	Size	Release Date	Downloaded	Currently Installed	Action
5.0.0	259 MB	2012/11/01 19:58:24	✔		Install
4.1.9	169 MB	2012/11/05 23:40:31			Download
4.1.8	168 MB	2012/09/22 21:01:08	✔	✔	Download
4.1.8-h3	168 MB	2012/10/18 23:49:21			Download
4.1.7	152 MB	2012/07/29			Download

Paso 5 Instale la actualización.

1. Haga clic en **Instalar**.
2. Reinicie Panorama:
   - Si se le pide que reinicie, haga clic en **Sí**.



   - Si no se le pide que reinicie, seleccione **Panorama > Configuración > Operaciones** y haga clic en **Reboot Panorama (Reiniciar Panorama)** en la sección Operaciones de dispositivo de la pantalla.

Paso 6 (Solo necesario para dispositivos virtuales de Panorama que se actualicen a la versión 5.1 de Panorama) Modifique la configuración del dispositivo virtual de Panorama.

Importante: Antes de activar un dispositivo virtual de Panorama a la versión 5.1, asegúrese de que el host ESX(i) admite un sistema operativo de 64 bits y que cumple los requisitos mínimos del sistema para el sistema operativo de 64 bits. Consulte Requisitos para obtener más información.

Después de que se reinicie Panorama, realice las siguiente tareas:

1. Desactive el dispositivo virtual.
2. Haga clic en el botón derecho y seleccione **Editar configuración...** para modificar estos parámetros:
   a. En la pestaña Options (Opciones), cambie el sistema operativo de invitado de **Other Linux (32-bit) (Otro Linux, 32 bits)** a **Other Linux (64-bit) (Otro Linux, 64 bits)**.
   b. En la pestaña Hardware, cambie el controlador SCSI de **BusLogic Parallel (Paralelo bus lógico)** a **LSI Logic Parallel (Paralelo lógico LSI)**.
   c. En la pestaña Hardware, cambie la asignación de memoria a 4 GB como mínimo; 16 GB para gestionar 10 o más cortafuegos.
3. Active el dispositivo virtual de Panorama.

Para continuar con la gestión de los cortafuegos y activar la recopilación de logs, consulte el Capítulo 3, Gestión de cortafuegos y recopilación de logs.

Navegación en la interfaz de usuario de Panorama

Panorama proporciona tres interfaces de usuario: una interfaz web, una interfaz de línea de comandos (CLI) y una API REST de gestión.

- Interfaz web: la interfaz web de Panorama está diseñada para parecerse al cortafuegos. Si ya conoce el cortafuegos, podrá navegar y completar tareas administrativas y generar tareas de informes desde la interfaz web de Panorama con relativa facilidad. Esta interfaz gráfica le permite acceder a Panorama con HTTPS y es la mejor forma de realizar tareas administrativas. Puede habilitar el acceso HTTP a Panorama, si se le solicita en la sección Configuración de interfaz de gestión en la pestaña **Panorama > Configuración > Management (Gestión)**. Consulte Navegación en la interfaz web y Inicio de sesión en la interfaz web.
- Interfaz de línea de comandos: la interfaz de línea de comandos (CLI) es una interfaz sencilla que le permite introducir los comandos con rapidez para completar una serie de tareas. La CLI admite dos modos de comandos (operativos y de configuración), cada uno de los cuales con su propia jerarquía de comandos e instrucciones. Cuando conoce la estructura de anidamiento y la sintaxis de los comandos, la CLI permite tipos de respuesta rápidos y ofrece eficacia administrativa. Consulte Inicio de sesión en la CLI.
- API REST de gestión: la API REST basada en XML se proporciona como servicio web implementado usando solicitudes y respuestas de HTTP/HTTPS . Le permite dinamizar las operaciones e integrarse con las aplicaciones y repositorios existentes desarrollados internamente. Para obtener más información sobre cómo utilizar la interfaz API de Panorama, consulte el documento PAN-OS and Panorama XML-Based REST API (API Rest basada en XML de PAN-OS). Para acceder a la comunidad en línea para desarrollar secuencias de comandos, visite: https://live.paloaltonetworks.com/community/devcenter

Navegación en la interfaz web

Use la interfaz web de Panorama para configurar Panorama, gestionar y supervisar los dispositivos gestionados y los recopiladores de logs y acceder a la interfaz web de todos los dispositivos web gestionados que usen el contexto de dispositivo. Consulte la ayuda en línea de Panorama para obtener detalles sobre las opciones de cada pestaña de la interfaz web.

La interfaz web de Panorama incluye las siguientes pestañas:

Pestaña	Pestaña secundaria	Descripción
Panel		Muestra información general sobre la configuración de acceso de red y el modelo de Panorama. Incluye widgets que muestran información sobre aplicaciones, logs, recursos y configuración del sistema.
ACC		Muestra el nivel de riesgo y amenaza general de la red, basado en información procedente de los dispositivos gestionados.
Supervisar		Proporciona acceso a logs e informes.

Pestaña	Pestaña secundaria	Descripción (Continuación)
Panorama		Configure Panorama, gestione licencias, establezca una alta disponibilidad, acceda a actualizaciones de software y alertas de seguridad y gestione los cortafuegos y recopiladores de logs implementados.
Grupos de dispositivos (Debe realizar la Creación de grupos de dispositivos para que aparezca esta pestaña.)	Políticas	Cree políticas centralizadas y aplique la configuración a varios grupos de dispositivos.
	Objetos	Defina objetos de política a los que se pueda hacer referencia en la política y que se puedan compartir en todos los grupos de dispositivos gestionados.
Plantillas (Debe realizar la Adición de una nueva plantilla para que aparezca esta pestaña.)	Red	Establezca la configuración de red, como los perfiles de red, que se puede aplicar a los dispositivos gestionados.
	Dispositivo	Establezca la configuración de red del dispositivo, como los perfiles de red y las funciones de administrador, que se puede aplicar a los dispositivos gestionados.

Inicio de sesión en la interfaz web

INICIO DE SESIÓN EN LA INTERFAZ WEB		
Paso 1.	Inicie sesión en la interfaz web de Panorama.	Si usa una conexión segura (https) desde un navegador web, inicie sesión usando la dirección IP y la contraseña que asignó durante la configuración inicial (https://<*dirección IP*>).
Paso 2	(Opcional) Habilitación del acceso HTTP y SSH.	1. Seleccione **Panorama > Configuración > Gestión** y, a continuación, haga clic en el icono Editar de la sección Configuración de interfaz de gestión de la pantalla. 2. Seleccione los servicios de gestión que permitirá en la interfaz. Por ejemplo, seleccione **HTTP** y **SSH**. 3. Haga clic en **ACEPTAR**.

Inicio de sesión en la CLI

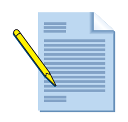
Puede iniciar sesión en la CLI de Panorama usando una conexión de puerto de serie o acceder remotamente usando un cliente de SSH.

INICIO DE SESIÓN EN LA CLI	
• Utilice SSH para iniciar sesión en la CLI de Panorama. **Nota** Se aplican las mismas instrucciones para un dispositivo M-100 en el modo de recopilación de logs.	1. Asegúrese de contar con lo siguiente: • Un ordenador con acceso de red a Panorama • Dirección IP de Panorama • SSH está activado en la interfaz de gestión. Para habilitar el acceso SSH, consulte (Opcional) Habilitación del acceso HTTP y SSH. 2. Para acceder a la CLI usando SSH: a. Introduzca la dirección IP de Panorama en el cliente SSH. b. Utilice el puerto 22. c. Introduzca las credenciales de acceso administrativo cuando se le soliciten. Después de iniciar la sesión correctamente, aparece el mensaje de la CLI en modo operativo. Por ejemplo: `admin@ABC_Sydney>` Para habilitar la autenticación basada en claves, consulte Activación de la autenticación basada en claves de SSH para la interfaz de la línea de comandos.
• Cambie al modo de configuración.	Para ir al modo de configuración, introduzca el siguiente comando en el mensaje: `admin@ABC_Sydney>` **`configure`** El mensaje cambia a `admin@ABC_Sydney#`
• Utilice un puerto de serie para iniciar sesión en la CLI de Panorama.	1. Asegúrese de contar con lo siguiente: • Un cable serie de módem nulo que conecta Panorama a un ordenador con un puerto de serie DB-9 • Un programa de emulación de terminal instalado en el ordenador 2. Utilice la siguiente configuración en el software de emulación para conectar: 9600 baudios, 8 bits de datos, 1 bit de terminación, sin paridad, sin control de flujo del hardware. 3. Introduzca las credenciales de acceso administrativo cuando se le soliciten.

Configuración del acceso administrativo

De forma predeterminada, Panorama incluye una cuenta administrativa predeterminada (admin) con acceso completo de lectura-escritura a todas las funcionalidades de Panorama. Es recomendable que cree una cuenta administrativa diferente para cada persona que necesite acceder a las funciones de administración o informes de Panorama Esto evita la configuración no autorizada (o modificación) y permite el registro de acciones de cada uno de los administradores.

Panorama le permite definir y restringir el acceso de forma tan amplia o limitada como necesite, según los requisitos de seguridad de la organización. Por ejemplo, puede decidir que el administrador de un centro de datos tenga acceso a toda la configuración de los dispositivos o la red, que un administrador de seguridad pueda tener control sobre la definición de la política de seguridad, el visor de log y la creación de informes y que otras personas concretas tengan acceso limitado a la CLI o API XML.



No puede añadir una cuenta administrativa a un dispositivo M-100 en modo de recopilación de logs. Solo la cuenta de usuarios administrativos con el nombre de usuario predeterminado *admin* está disponible.

En las siguientes secciones se describen los diversos métodos de configurar cuentas administrativas y ofrecen procedimientos para configurar accesos administrativos básicos:

- Creación de una cuenta administrativa
- Definición de los dominios de acceso
- Definición de una secuencia de autenticación
- Definición de los dominios de acceso
- Configuración de la autenticación administrativa; para obtener información sobre las distintas opciones disponibles para autenticar usuarios administrativos, consulte Autenticación administrativa.

Creación de una cuenta administrativa

Los usuarios administrativos deben contar con una cuenta y tener asignada una *función*. La función define el tipo de acceso que el administrador asociado tiene en Panorama; puede asignar el usuario administrativo a una función dinámica integrada o a una función personalizada (Perfil de función de administrador) que defina. Si pretende usar perfiles de funciones de administrador en lugar de funciones dinámicas, cree los perfiles que definan qué tipo de acceso, de haberlo, se dará a las diferentes secciones de la interfaz web, CLI y API XML para cada administrador asignado a la función. Si desea más información sobre funciones, consulte Funciones administrativas.

Puede definir también la complejidad mínima de la contraseña para cada usuario administrativo, así como un perfil de contraseña y usar un perfil de autenticación para utilizar un servicio de autenticación externo para validar las credenciales del administrador.

El siguiente ejemplo muestra el modo de crear una cuenta de administrador local con autenticación local:

CREACIÓN DE UNA CUENTA DE ADMINISTRADOR LOCAL	
Paso 1. Cree un perfil de función de administrador. Este paso solo es necesario se utiliza funciones personalizadas en lugar de funciones dinámicas disponibles en Panorama.	Complete los siguientes pasos para cada función que desee crear: 1. Seleccione **Panorama > Funciones de administrador** y, a continuación, haga clic en **Añadir**. 2. Seleccione **Panorama** o **Grupo de dispositivos y Plantilla** para definir el ámbito de los privilegios administrativos que se deben asignar. Los privilegios de acceso definidos para Panorama entran en vigor cuando el administrador inicia sesión en Panorama, la función Grupo de dispositivos y Plantilla aplica el acceso de solo lectura a los dispositivos gestionados, plantillas y nodos de grupos de dispositivos de la pestaña **Panorama**. El acceso al resto de pestañas se puede modificar según sea necesario. 3. En las pestañas **Interfaz web** o **API XML**, establezca los niveles de acceso (Habilitar**,** Solo lectura, Deshabilitar) de cada área funcional de la interfaz haciendo clic en el icono para cambiarlo a la configuración deseada: • Para acceder a Panorama, defina el acceso a **Interfaz web**, **API XML** y **Línea de comandos**. La pestaña **Línea de comandos** no permite el acceso restringido. Debe seleccionar una de las opciones predefinidas: **superusuario, superlector, administrador de Panorama** o **Ninguno**. • Para acceder a los cortafuegos (Grupo de dispositivos y Plantilla), solo hay disponible una pestaña: **Interfaz web.** Desde Panorama no se puede habilitar el acceso a la interfaz CLI o API XML en un dispositivo porque no hay funciones predefinidas que restrinjan el acceso. Por lo tanto, para evitar el escalamiento de niveles de privilegios, no existe la posibilidad de gestionar el acceso a la CLI y API XML desde Panorama. 4. Introduzca un **nombre** para el perfil y haga clic en **Aceptar** para guardarlo.
Paso 2 (Opcional) Establezca requisitos para contraseñas definidas por usuarios locales.	• **Crear perfiles de contraseña**: Defina la frecuencia con que los administradores deberán cambiar sus contraseñas. Puede crear varios perfiles de contraseña y aplicarlos a las cuentas de administrador según sea necesario para imponer la seguridad deseada. Para crear un perfil de la contraseña, seleccione **Panorama > Perfiles de la contraseña** y, a continuación, haga clic **Añadir**. • **Configurar ajustes de complejidad mínima de la contraseña**: define las reglas que rigen la complejidad de la contraseña, lo que fuerza a los administradores a crear contraseñas que sean más difíciles de descifrar o evitar. Al contrario de lo que pasa en los perfiles de contraseñas, que se pueden aplicar a cuentas individuales, estas reglas se aplican a todo el dispositivo y a todas las contraseñas. Para configurar los ajustes, seleccione **Panorama > Configuración** y, a continuación, haga clic en el icono Editar de la sección Complejidad de contraseña mínima.

CREACIÓN DE UNA CUENTA DE ADMINISTRADOR LOCAL (CONTINUACIÓN)		
Paso 3	Cree una cuenta para cada administrador.	1. Seleccione **Panorama > Administradores** y, a continuación, haga clic en **Añadir**. 2. Introduzca un **nombre** y **contraseña** para el administrador. 3. Seleccione la **función** que se asignará a este administrador. Seleccione una función dinámica o un perfil basado en funciones personalizadas como se estableció en el Paso 1. 4. (Opcional) Seleccione el **perfil de autenticación** que se debe utilizar para validar las credenciales de un usuario administrativo en un servidor de autenticación externo. Consulte Creación de un perfil de autenticación. 5. (Opcional) Seleccione un **perfil de contraseña**. Consulte Paso 2. 6. Haga clic en **Aceptar** para guardar la cuenta.
Paso 4	Guarde los cambios de configuración.	7. Haga clic en **Compilar** y seleccione **Panorama** en la opción **Compilar tipo**.

Definición de los dominios de acceso

Un *dominio de acceso* es una forma de limitar el acceso administrativo a los grupos de dispositivos especificados (para gestionar políticas y objetos) y a las plantillas (para gestionar ajustes de la red y dispositivos) y ofrece la posibilidad de cambiar el contexto en la interfaz web de los dispositivos gestionados. Los ajustes de dominio de acceso solo son relevantes si:

- Se ha definido un perfil de función de administrador personalizada con una función **Grupo de dispositivos y Plantilla**.
- Se utiliza un servidor RADIUS para la autenticación del administrador. El dominio de acceso está vinculado a atributos específicos del proveedor (VSA) RADIUS. Se ha definido un número de atributo VSA y el valor para cada usuario administrativo en el servidor RADIUS. El valor definido debe coincidir con el dominio de acceso configurado en Panorama. Cuando un administrador intenta iniciar sesión en Panorama, Panorama consulta al servidor RADIUS el dominio de acceso del administrador y el número de atributo. Basándose en la respuesta del servidor RADIUS, se autoriza el acceso del administrador, restringiéndolo a los sistemas virtuales/de dispositivos, grupos de dispositivos y plantillas especificadas en el dominio de acceso. Para obtener detalles de los VSA de RADIUS, consulte Uso de los atributos específicos de proveedor (VSA) de RADIUS.

DEFINICIÓN DE UN DOMINIO DE ACCESO		
Paso 1.	Cree un dominio de acceso.	1. Seleccione **Panorama > Dominio de acceso** y, a continuación, haga clic en **Añadir**. 2. Introduzca un **nombre** de usuario para identificar el dominio.
Paso 2	Especifique los grupos de dispositivos, plantillas y contextos de dispositivos que el usuario puede administrar.	En las pestañas **Grupos de dispositivos**, **Plantillas** y **Contexto de dispositivo**, haga clic en **Añadir** y elija en la lista filtrada o desplegable que aparece.
Paso 3	Guarde los cambios de configuración.	Haga clic en **Compilar** y seleccione **Panorama** en la opción **Compilar tipo**.

Creación de un perfil de autenticación

Un perfil de autenticación especifica el servicio de autenticación que valida las credenciales del administrador y define cómo acceder a dicho servicio. Panorama se puede configurar para acceder a la base de datos local, a un servidor RADIUS, servidor Kerberos o a un servidor LDAP.

Si utiliza un servidor de autenticación externo, cree un perfil de servidor (**Panorama > Perfiles de servidor**) antes de crear un perfil de autenticación. Panorama necesita que el perfil del servidor acceda al servicio de autenticación.

CREACIÓN DE UN PERFIL DE AUTENTICACIÓN		
Paso 1.	Cree un perfil de autenticación.	1. Seleccione **Panorama > Perfil de autenticación** y, a continuación, haga clic en **Añadir**. 2. Introduzca un **nombre** de usuario para identificar un perfil de autenticación.
Paso 2	Defina las condiciones para bloquear al usuario administrativo.	1. Introduzca el **tiempo de bloqueo**. Este es el número de minutos que se bloquea a un usuario cuando alcanza el número máximo de intentos fallidos ((0-60 minutos; de forma predeterminada es 0). 0 significa que el bloqueo continuará mientras que no se desbloquee manualmente. 2. Introduzca el valor en **Intentos fallidos**. Número de intentos de inicio de sesión fallidos que se permiten antes de bloquear la cuenta (1-10; de forma predeterminada es 0). De forma predeterminada, el número de intentos fallidos es 0, por lo que no se bloquea al usuario aunque la autenticación falle repetidamente.
Paso 3	Especifique a los usuarios y grupos que tienen permiso explícito para autenticar. Puede limitar el acceso a usuarios específicos de un grupo/directorio de usuarios añadiendo una lista permitida en un perfil de autenticación.	Para la **Lista de permitidas**, elija una de las siguientes opciones: • Seleccione la casilla de verificación **Todos** para permitir a todos los usuarios. • Haga clic en **Añadir** e introduzca los primeros caracteres de un nombre en el campo para que aparezca una lista de todos los usuarios y grupos de usuarios que empiezan por esos caracteres. Repita el proceso para añadir tantos usuarios/grupos de usuarios como sea necesario.
Paso 4	Seleccione el servicio de autenticación y adjunte el perfil del servidor.	1. En el menú desplegable **Autenticación**, seleccione el tipo de autenticación que utilizará. 2. Seleccione el perfil de usuario adecuado en el menú desplegable **Perfil de servidor**.
Paso 5	Confirme los cambios.	Haga clic en **Compilar** y seleccione **Panorama** en la opción **Compilar tipo**.

Lockout						
Failed Attempts (#)	Lockout Time (min)	Allow List	Authenticat...	Server Profile	Others	Locked Users
default	default	all	RADIUS	MJS-RADIUS		none

Definición de una secuencia de autenticación

Una secuencia de autenticación es una lista ordenada de perfiles de autenticación que permite el uso de varios servicios de autenticación. Las secuencias de autenticación proporcionan flexibilidad en entornos con varias bases de datos para distintos usuarios y grupos de usuarios. Cuando se define una secuencia de autenticación, Panorama intenta autenticar al administrador usando todos los perfiles de servidor configurados en secuencia. Por ejemplo, una secuencia de autenticación puede indicar a Panorama que compruebe el LDAP en primer lugar, después RADIUS y la base de datos local en último lugar, hasta que se produzca una autenticación correcta; si falla, se impide el acceso del administrador.

DEFINICIÓN DE UNA SECUENCIA DE AUTENTICACIÓN		
Paso 1.	Cree una secuencia de autenticación.	1. Seleccione **Panorama > Secuencia de autenticación** y, a continuación, haga clic en **Añadir**. 2. Introduzca un **nombre** de usuario para identificar la secuencia de autenticación. 3. Haga clic en **Añadir** para seleccionar la secuencia cronológica de perfiles de autenticación en los que deben comprobarse las credenciales del administrador.
Paso 2	(Opcional) Defina las condiciones para bloquear al usuario administrativo.	1. Introduzca el **tiempo de bloqueo**. Este es el número de minutos que se bloquea a un usuario cuando alcanza el número máximo de intentos fallidos ((0-60 minutos; de forma predeterminada es 0). 0 significa que el bloqueo continuará mientras que no se desbloquee manualmente. 2. Introduzca el valor en **Intentos fallidos**. Número de intentos de inicio de sesión fallidos que se permiten antes de bloquear la cuenta (1-10; de forma predeterminada es 0). De forma predeterminada, el número de intentos fallidos es 0, por lo que no se bloquea al usuario aunque la autenticación falle repetidamente.
Paso 3	Guarde los cambios de configuración.	Haga clic en **Compilar** y seleccione **Panorama** en la opción **Compilar tipo**.

Configuración de la autenticación administrativa

Los administradores se pueden autenticar localmente en Panorama usando contraseñas o certificados o se pueden autenticar en un servidor de autenticación externo.

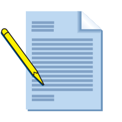
Hay tres alternativas para configurar la autenticación administrativa en Panorama:

▲ Crear una cuenta de usuario local y realizar la autenticación localmente usando una contraseña o mediante un certificado o clave. Consulte Creación de una cuenta administrativa; Activación de la autenticación basada en certificado para la interfaz web y Activación de la autenticación basada en claves de SSH para la interfaz de la línea de comandos.

- ▲ Crear una cuenta de usuario local pero realizar la autenticación en un servidor RADIUS/LDAP/Kerberos externo usando perfiles de autenticación:
  - – Crear un perfil de servidor en la pestaña **Panorama > Perfil de servidor**. Se necesita un perfil de servidor para cada servicio externo con el que deba interactuar Panorama. Los detalles del servidor necesarios para establecer la conexión con Panorama varían según el servicio de autenticación que planee utilizar.
  - – Cree un perfil de autenticación. Consulte Creación de un perfil de autenticación.
  - – (Solo acceso basado en función) Defina un perfil de función de administrador que especifique si el usuario tiene acceso a Panorama o a Grupos de dispositivos y plantillas; consulte Cree un perfil de función de administrador. Para las funciones dinámicas no se necesita ningún perfil de función administrativa.
- ▲ Utilice los atributos específicos de proveedor (VSA) de RADIUS para gestionar el acceso administrativo en Panorama. Utilice esta opción si no desea crear una cuenta local en Panorama para un usuario administrativo y desea utilizar la infraestructura actual para gestionar la autenticación y la contraseña en un servidor RADIUS. Para obtener una visión general de alto nivel del proceso, consulte Uso de los atributos específicos de proveedor (VSA) de RADIUS.

Activación de la autenticación basada en certificado para la interfaz web

Una alternativa más segura al uso de contraseña para autenticar a un usuario es activar la autenticación basada en certificado para asegurar el acceso a Panorama. Con la autenticación basada en certificado se intercambia y verifica una firma, en lugar de una contraseña.



Para activar la autenticación basada en certificado, debe configurar un perfil de certificado de cliente (consulte el Paso 4 y el Paso 5). Cuando activa un perfil de certificado de cliente, todos los administradores deben usar un certificado de cliente para acceder a Panorama.

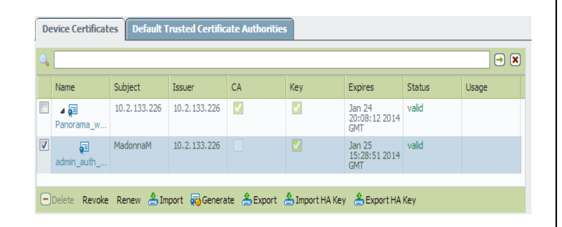
Utilice las siguientes instrucciones para activar la autenticación basada en certificado. En este ejemplo se utiliza un certificado de CA generado en Panorama.

ACTIVACIÓN DE LA AUTENTICACIÓN BASADA EN CERTIFICADO	
Paso 1. Genere un certificado de CA en Panorama. **Nota** Para usar un certificado de un CA de terceros o de una empresa, debe importar ese certificado de CA a Panorama.	Para generar un certificado de CA en Panorama: 1. Inicie sesión en la interfaz web de Panorama. 2. Seleccione **Panorama > Gestión de certificados > Certificados** y haga clic en **Generar**. 3. Introduzca un **nombre de certificado**. Agregue la dirección IP o FQDN de Panorama para que aparezca en el campo **Nombre común** del certificado. Opcionalmente, puede cambiar los ajustes criptográficos y definir las opciones de certificados como el país, la organización y el estado. 4. Asegúrese de dejar en blanco la opción **Firmado por** y seleccionar la opción **Autoridad del certificado**. 5. Haga clic en **Generar** para crear el certificado usando los detalles especificados anteriormente.

ACTIVACIÓN DE LA AUTENTICACIÓN BASADA EN CERTIFICADO (CONTINUACIÓN)

Paso 2 Cree y exporte el certificado del cliente que se utilizará para autenticar un administrador.

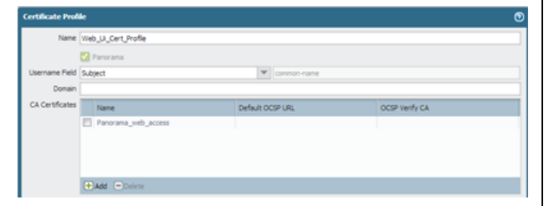




1. Utilice el certificado de CA para generar un certificado de cliente para el usuario administrativo especificado.
   a. Seleccione **Panorama > Gestión de certificados > Certificados** y haga clic en **Generar**.
   b. En el campo **Nombre común**, introduzca el nombre del administrador para el que está generando el certificado. La sintaxis del nombre debe coincidir con el formato usado por el mecanismo de autenticación local o externo.
   c. En el campo **Firmado por**, seleccione el mismo certificado de CA creado en el Paso 1.
   d. Haga clic en **Generar** para crear el certificado.
2. Exporte el certificado del cliente que acaba de generar.
   a. Seleccione el certificado que acaba de generar y haga clic en **Exportar**.
   b. Para cifrar la clave privada, seleccione **PKCS12** como **formato de archivo**.
   c. Introduzca una frase de contraseña para cifrar la clave privada y confirmar la entrada.
   d. Haga clic en **Aceptar** para exportar el certificado.

Paso 3 Cree o modifique una cuenta de administrador para activar el certificado del cliente en la cuenta.

1. Seleccione **Panorama > Administradores** y, a continuación, haga clic en **Añadir**.
2. Introduzca un nombre de inicio de sesión para el administrador; el nombre distingue entre mayúsculas y minúsculas.
3. Seleccione **Utilizar únicamente el certificado de autenticación de cliente (web)** para activar el uso del certificado para la autenticación.
4. Seleccione la **función** que se asignará a este administrador. Puede seleccionar una de las funciones dinámicas predefinidas o seleccionar una función personalizada y adjuntar un perfil de autenticación que especifique los privilegios de acceso para este administrador.
5. (Opcional) Para funciones personalizadas, seleccione los grupos de dispositivos, las plantillas y el contexto del dispositivo que el usuario administrativo puede modificar.
6. Haga clic en **ACEPTAR** para guardar los ajustes de la cuenta.

ACTIVACIÓN DE LA AUTENTICACIÓN BASADA EN CERTIFICADO (CONTINUACIÓN)		
Paso 4	Cree el perfil del certificado que se utilizará para asegurar el acceso a la interfaz web.  	1. Seleccione **Panorama > Gestión de certificados > Perfil del certificado** y haga clic en **Añadir**. 2. Introduzca un nombre para el perfil del certificado y en **Campo de nombre de usuario** seleccione **Asunto**. 3. Seleccione **Añadir** en la sección de certificados de CA y en el menú **Certificado de CA**, seleccione el certificado de CA creado en el Paso 1.
Paso 5	Configure Panorama para que utilice el perfil del certificado del cliente para la autenticación.	1. En la pestaña **Panorama > Configuración**, haga clic en el icono Editar de la sección Configuración de autenticación de la pantalla. 2. En el campo **Perfil del certificado**, seleccione el perfil del certificado del cliente creado en el Paso 4. 3. Haga clic en **ACEPTAR** para guardar los cambios.
Paso 6	Guarde los cambios de configuración.	Haga clic en **Compilar** y seleccione **Panorama** como **Compilar tipo**. Se cerrará su sesión del dispositivo.
Paso 7	Importe el certificado del cliente del administrador en el navegador web del sistema cliente que el administrador utilizará para acceder a la interfaz web de Panorama.	Por ejemplo, en Firefox: 1. Seleccione **Tools (Herramientas) > Options (Opciones) > Avanzado**. 2. Haga clic en **View Certificates (Ver certificados)**. 3. Seleccione la pestaña **Your Certificates (Sus certificados)** y haga clic en **Importar**. Acceda a la ubicación en la que ha guardado el certificado del cliente. 4. Cuando se le solicite, introduzca la frase de contraseña para descifrar la clave privada.
Paso 8	Compruebe que se ha configurado la autenticación basada en certificado.	1. Desde un sistema cliente con el certificado del cliente cargado, acceda a la dirección IP o nombre de host de Panorama. 2. Cuando se le solicite, seleccione el certificado cliente que ha importado en el Paso 7. Aparecerá una advertencia de certificación. 3. Añada el certificado a la lista de excepciones e inicie sesión en la interfaz web de Panorama.

Activación de la autenticación basada en claves de SSH para la interfaz de la línea de comandos

Para activar la autenticación basada en claves de SSH, complete el siguiente flujo de trabajo para cada usuario administrativo:

ACTIVACIÓN DE LA AUTENTICACIÓN (BASADA EN CLAVE PÚBLICA) DE SSH		
Paso 1.	Utilice una herramienta de generación de claves de SSH para crear un par de claves asimétricas en la máquina cliente. Los formatos de clave admitidos son: IETF SECSH y Open SSH; los algoritmos admitidos son: DSA (1024 bits) y RSA (768-4096 bits).	Para saber los comandos necesarios para generar el par de claves, consulte la documentación del producto para el cliente de SSH. La clave pública y la privada son dos archivos diferentes; guárdelos ambos en una ubicación a la que Panorama pueda acceder. Para una mayor seguridad, introduzca una frase de contraseña para cifrar la clave privada. Al administrador se le pedirá esta frase de contraseña cuando inicie sesión en Panorama.
Paso 2	Cree una cuenta para el administrador y permita la autenticación basada en certificado.	1. Seleccione **Panorama > Administradores** y, a continuación, haga clic en **Añadir**. 2. Introduzca un **nombre** y **contraseña** para el administrador. Asegúrese de introducir una contraseña fuerte o compleja y guárdela en un lugar seguro; Panorama solo se la pedirá en caso de que los certificados estén dañados o que se produzca un fallo del sistema. 3. (Opcional) Seleccione un **Perfil de autenticación**. 4. Habilite **Utilizar autenticación de clave pública (SSH).** 5. Haga clic en **Importar clave** y acceda a la clave pública creada en el Paso 1. 6. Seleccione la **función** que se asignará a este administrador. Puede seleccionar una de las funciones dinámicas predefinidas o un perfil basado en función personalizado. Para obtener más información, consulte Cree un perfil de función de administrador. 7. Haga clic en **ACEPTAR** para guardar la cuenta.
Paso 3	Guarde los cambios de configuración.	8. Haga clic en **Compilar** y seleccione **Panorama** como la opción de **Compilar tipo**.
Paso 4	Compruebe que el cliente SSH utiliza la clave privada para autenticar la clave pública presentada por Panorama.	1. Configure el cliente SSH para utilizar la clave privada para autenticar en Panorama. 2. Inicie sesión en la CLI de Panorama. [illegible] - PuTTY `login as: [illegible]` `Authenticating with public key "dsa-key-20130415"` `Passphrase for key "dsa-key-20130415":` `Last login: [illegible] 15:59:52 2013 from [illegible]` `Welcome [illegible]` 3. Si se le solicita, introduzca la frase de contraseña definida al crear las claves en el Paso 1.

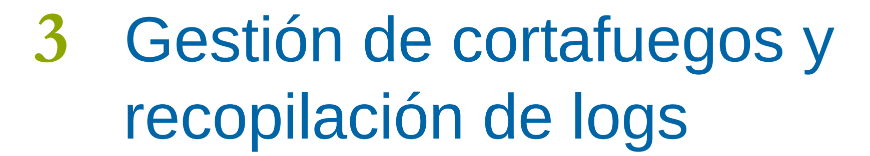
Uso de los atributos específicos de proveedor (VSA) de RADIUS

Para utilizar los VSA de RADIUS, debe completar las siguientes tareas:

- En Panorama:
  - Configure un perfil de servidor RADIUS (**Panorama > Perfiles de servidor > RADIUS**).
  - Cree un perfil de autenticación que especifique RADIUS como el protocolo de autenticación y adjunte el perfil de servidor RADIUS (**Panorama > Perfiles de autenticación**).
  - Cree un perfil de función administrativa personalizada con una función Grupo de dispositivos y Plantilla (**Panorama > Funciones de administrador**).
  - Configure Panorama para que utilice el perfil de autenticación para la misma (**Configuración > Gestión > Configuración de autenticación >Perfil de autenticación**).
  - (Solo necesario si utiliza los VSA: PaloAlto-Panorama-Admin-Access-Domain) Si desea limitar el acceso administrativo a dispositivos administrados, plantillas o grupos de dispositivos específicos, defina un dominio de acceso [**Panorama > Access Domains** (Dominios de acceso)].
- En el servidor RADIUS:
  - Añada la dirección IP o el nombre de host de Panorama como cliente de RADIUS.
  - Defina los VSA admitidos por Panorama. Para definir un atributo, utilice el código de proveedor (25461), el nombre de atributo (asegúrese de que coincide con el nombre del perfil de la función de administrador/dominio de acceso definido en Panorama; distingue entre mayúsculas y minúsculas), número, formato (cadena):
    - `PaloAlto-Panorama-Admin-Role, attribute #3`
    - `PaloAlto-Panorama-Admin-Access-Domain, attribute #4`

Para obtener instrucciones detalladas sobre cómo configurar la autenticación usando los VSA de RADIUS, consulte los siguientes documentos:

- En Windows 2003 Server y Cisco ACS 4.0: https://live.paloaltonetworks.com/docs/DOC-1765
- En Cisco ACS 5.2: https://live.paloaltonetworks.com/docs/DOC-1979



3 Gestión de cortafuegos y recopilación de logs

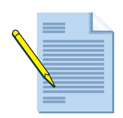
Panorama proporciona dos funciones principales: centraliza el proceso de administración de cortafuegos de Palo Alto Networks y ofrece visibilidad del tráfico de red a través de informes agregados. Para administrar los dispositivos y generar informes sobre el tráfico de red, debe añadir los cortafuegos a Panorama como dispositivos gestionados y configurar los cortafuegos para que reenvíen logs a Panorama o a un recopilador de logs. Esta sección incluye los siguientes temas:

- Gestión de sus cortafuegos
- Habilitación de logs
- Implementación de actualizaciones de software y gestión de licencias
- Sustitución de un dispositivo gestionado por un nuevo dispositivo, para sustituir un dispositivo de autorización de devolución de mercancía
- Transición de un dispositivo a una gestión central

Gestión de sus cortafuegos

Como Panorama está diseñado para ser un punto clave en la administración de cortafuegos, el flujo de trabajo de este documento es más adecuado para un cortafuegos que se implemente por primera vez. Revise Planificación de su implementación y luego continúe con las siguientes secciones:

- ▲ Adición de dispositivos gestionados
- ▲ Creación de grupos de dispositivos
- ▲ Creación de plantillas
- ▲ Configuración de los cortafuegos para reenviar logs a Panorama
- ▲ Compilación de cambios en Panorama
- ▲ Modificación de los valores predeterminados de almacenamiento en búfer y reenvío de logs
- ▲ Uso de Panorama para configurar dispositivos gestionados: ejemplo



Para ver las pestañas **Objects (Objetos), Políticas** en la interfaz web de Panorama, primero debe crear como mínimo un grupo de dispositivos y como mínimo una plantilla para que aparezcan las pestañas **Red** y **Dispositivo**. Estas pestañas incluyen las opciones de configuración necesarias para configurar y gestionar los cortafuegos de su red.

Si ya ha configurado e implementado cortafuegos en su red, el proceso de migrar la configuración, las políticas locales y los objetos desde los cortafuegos a un enfoque de gestión centralizado requiere comprender las secuencias de comandos y el uso de la API REST en los cortafuegos. Para que esta transición sea eficaz, Palo Alto Networks recomienda utilizar socios cualificados y certificados que estén familiarizados con las etapas de planificación, implementación y verificación del proceso de migración. Póngase en contacto con su socio o distribuidor autorizado para obtener más información sobre las ofertas de asistencia técnica que tiene a su disposición. Para obtener una breve descripción general del proceso, consulte Transición de un dispositivo a una gestión central y para obtener información más detallada, consulte este artículo: Panorama Device Migration Tech Note (Nota técnica sobre migración de dispositivos de Panorama).

Adición de dispositivos gestionados

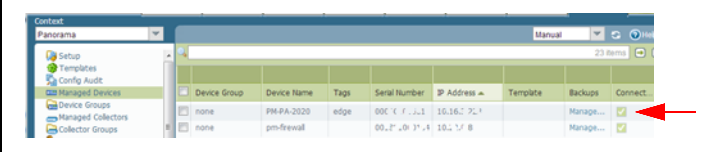
La adición de cortafuegos a Panorama es el primer paso para gestionarlos de manera central mediante Panorama. Antes de comenzar, recopile los números de serie de todos los dispositivos que desee gestionar con Panorama.

Para gestionar un cortafuegos con Panorama, prepare cada cortafuegos de la siguiente manera:

- Realice una configuración inicial en el cortafuegos para que el dispositivo sea accesible y pueda comunicarse con Panorama a través de la red.
- Añada las direcciones IP de Panorama (un servidor o dos, si Panorama tiene configurado un clúster en alta disponibilidad) en la sección Ajustes de Panorama de la pestaña **Dispositivo > Configuración > Gestión** y compile los cambios.

- Configure las interfaces de datos. Para cada interfaz que tenga la intención de utilizar, seleccione el tipo de interfaz y adjúntelo a una zona de seguridad para que pueda introducir la configuración y la política desde Panorama.

A continuación, podrá añadir los cortafuegos como dispositivos gestionados en Panorama de la manera siguiente:

ADICIÓN DE DISPOSITIVOS PARA SU GESTIÓN	
Paso 1. Añada dispositivos a Panorama.	1. Seleccione **Panorama > Dispositivos gestionados**. 2. Haga clic en **Añadir** e introduzca el número de serie de cada dispositivo que desee gestionar centralmente mediante Panorama. Añada únicamente una entrada por línea. 3. Haga clic en **ACEPTAR**. Los dispositivos recién añadidos aparecerán en el panel Dispositivos gestionados. 4. (Opcional) Añada una **Etiqueta**. Las etiquetas le facilitan buscar un dispositivo en una lista de gran tamaño; le ayudan a filtrar dinámicamente y ajustar la lista de cortafuegos que se muestra. Por ejemplo, si añade una etiqueta denominada sucursal, podrá filtrar todos los dispositivos de sucursal de su red. a. Seleccione la casilla de verificación que se encuentra junto al dispositivo gestionado. b. Haga clic en **Etiqueta** Tag . Haga clic en **Añadir** e introduzca una cadena de texto de hasta 31 caracteres. No utilice espacios en blanco. c. Haga clic en **ACEPTAR**. 5. Haga clic en **Compilar** y seleccione **Panorama** como **Compilar tipo**.
Paso 2 Verifique que el dispositivo está conectado a Panorama.	Si se puede acceder al cortafuegos en la red y la dirección IP de Panorama está configurada en el dispositivo, Panorama debe poder conectarse ( ) al dispositivo. 

Creación de grupos de dispositivos

Después de añadir los dispositivos, podrá agrupar los dispositivos en *grupos de dispositivos*. Un grupo de dispositivos puede incluir uno o más cortafuegos o sistemas virtuales que necesitan políticas y objetos similares y, por lo tanto, puede gestionarse eficazmente como una unidad lógica.

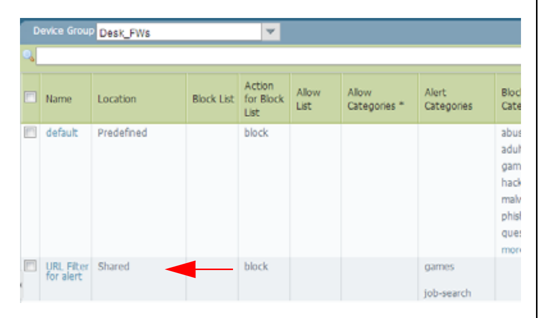
Al gestionar cortafuegos con una configuración de alta disponibilidad (HA) activa-pasiva, asegúrese de colocar ambos dispositivos en el mismo grupo de dispositivos en Panorama. Esto es esencial para asegurarse de que se introducen las mismas políticas y los mismos objetos en ambos dispositivos del clúster en HA. Las políticas introducidas por Panorama no se sincronizan entre peers de HA de cortafuegos.

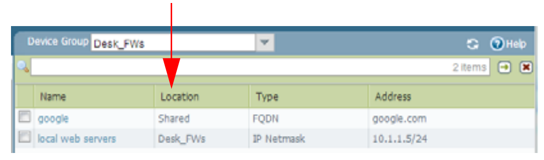
CREACIÓN DE GRUPOS DE DISPOSITIVOS	
Paso 1. Cree grupos de dispositivos. **Nota** Un dispositivo únicamente puede pertenecer a un grupo de dispositivos; en el caso de dispositivos con varios sistemas virtuales, cada sistema virtual puede pertenecer a un grupo de dispositivos diferente.	1. Seleccione **Panorama > Grupos de dispositivos** y haga clic en **Añadir**. 2. Introduzca un **Nombre** y una **Descripción** para identificar el grupo de dispositivos. 3. Utilice los filtros para seleccionar los dispositivos que desee añadir al grupo. 4. (Opcional) Seleccione la casilla de verificación **HA del peer de grupo** para cortafuegos que estén configurados como un clúster en HA. La adición de ambos dispositivos o sistemas virtuales al mismo grupo de dispositivos le permite introducir políticas y objetos compartidos simultáneamente en ambos peers. **Nota** Para agrupar peers de HA, los dispositivos deben ejecutar PAN-OS 5.0 o posterior. 5. (Opcional) Si tiene la intención de utilizar usuarios o grupos en una política, debe asignar un **Dispositivo principal** al grupo de dispositivos. El dispositivo principal es el cortafuegos desde el que Panorama recopila información de grupos de usuarios y nombres de usuarios para su uso en las políticas. 6. Haga clic en **ACEPTAR**. 7. Haga clic en **Compilar** y seleccione **Panorama** como **Compilar tipo**. Guarde los cambios en la configuración que se esté ejecutando en Panorama. 8. Haga clic en **Compilar** y seleccione **Grupo de dispositivos** como **Compilar tipo**. Introduzca los cambios en los dispositivos en el grupo de dispositivos.
Paso 2 Empiece a administrar centralmente las políticas en los dispositivos de los grupos de dispositivos.	• Creación de objetos para su uso en una política de grupo de dispositivos o compartida • Gestión de objetos compartidos • Dirección de políticas a un subconjunto de dispositivos • Visualización de jerarquía de reglas y búsqueda de reglas no utilizadas Para ver un ejemplo, consulte Uso de Panorama para configurar dispositivos gestionados: ejemplo

Creación de objetos para su uso en una política de grupo de dispositivos o compartida

Un *objeto* es un contenedor para agrupar identidades discretas, como direcciones IP, URL, aplicaciones o usuarios, para su uso en la aplicación de políticas. Puede utilizar Panorama para crear y duplicar todos los objetos de la pestaña **Objects (Objetos)** como **Dirección/Grupo de direcciones, Región o Usuario/Grupo de usuarios**. Estos objetos de políticas pueden compartirse entre todos los dispositivos gestionados o ser específicos de un grupo de dispositivos.

- Un *objeto compartido* es un componente reutilizable creado en Panorama. Se comparte entre todos los grupos de dispositivos y puede hacerse referencia a él en las políticas compartidas o las políticas de grupo de dispositivos. Reduce la carga administrativa y garantiza la coherencia al configurar varios cortafuegos.
- Un objeto de *grupo de dispositivos* es específico del grupo de dispositivos en el que se defina. Únicamente puede utilizarse en el grupo de dispositivos en el que se haya creado y no es visible al configurar otros grupos de dispositivos o reglas y objetos compartidos. Por ejemplo, un objeto de grupo de dispositivos para un conjunto de direcciones IP de servidor web creado en el grupo de dispositivos de centro de datos no está disponible para su uso en ningún otro grupo de dispositivos o para su uso en políticas compartidas.

CREACIÓN DE OBJETOS	
Cree un objeto compartido. En este ejemplo, añadiremos un objeto compartido a categorías de filtrado de URL en las que queramos activar una alerta. 	1. Seleccione la pestaña **Objects (Objetos) > Perfiles de seguridad > Filtrado de URL** y haga clic en **Añadir.** Si la pestaña **Objects (Objetos)** no aparece, consulte Adición de dispositivos gestionados para añadir un grupo de dispositivos. La interfaz web de Panorama muestra la pestaña **Objects (Objetos)** únicamente si ha creado un grupo de dispositivos.
	2. Introduzca un **Nombre** y una **Descripción**.
	3. Seleccione la casilla de verificación **Compartido**. Si no selecciona la casilla de verificación, el objeto formará parte del grupo de dispositivos que se muestra actualmente en la lista desplegable **Grupo de dispositivos**.
	4. Seleccione la casilla de verificación que aparece junto a las **Categorías de URL** para las que desea recibir una notificación y seleccione **Alerta** en la columna **Acción**; a continuación, haga clic en **ACEPTAR**.
	5. Haga clic en **Compilar** y seleccione **Panorama** como **Compilar tipo**.

CREACIÓN DE OBJETOS (CONTINUACIÓN)	
Cree un objeto de grupo de dispositivos. En este ejemplo, añadiremos un objeto de grupo de dispositivos para los servidores web específicos de su red.	1. Seleccione el grupo de dispositivos para el que tiene la intención de utilizar este objeto en la lista desplegable **Grupo de dispositivos**. 2. Seleccione la pestaña **Objects (Objetos) > Direcciones.** 3. Seleccione **Dirección** y haga clic en **Añadir**. 4. Verifique que la casilla de verificación **Compartido** no está seleccionada. 5. Introduzca un **Nombre** y una **Descripción** y seleccione el **Tipo** de objeto de dirección en la lista desplegable. Por ejemplo, seleccione **Intervalo de IP** e incluya el intervalo de direcciones IP de los servidores web para los que desee crear un objeto de dirección. 6. Haga clic en **ACEPTAR**. 7. Compile los cambios. a. Haga clic en **Compilar** y seleccione **Panorama** como **Compilar tipo**. Esto guardará los cambios en la configuración que se esté ejecutando en Panorama. b. Haga clic en **Compilar** y seleccione **Grupo de dispositivos** como **Compilar tipo**. Esto introducirá los cambios en los dispositivos en el grupo de dispositivos.
Visualice los objetos compartidos y los objetos de grupo de dispositivos en Panorama. Para mostrar la diferencia entre un objeto compartido y un objeto de grupo de dispositivos, la siguiente captura de pantalla incluye un objeto de dirección compartido creado en Panorama. 	La columna **Ubicación** de la pestaña **Objects (Objetos)** muestra si un objeto es compartido o específico para un grupo de dispositivos. 1. Seleccione el grupo de dispositivos, para el que acaba de crear un objeto de grupo de dispositivos, en la lista desplegable **Grupo de dispositivos**. 2. Seleccione la pestaña **Objects (Objetos) > Direcciones** y verifique que aparece el objeto de grupo de dispositivos; tenga en cuenta que el nombre del grupo de dispositivos de la columna Ubicación coincide con la selección en la lista desplegable **Grupo de dispositivos**. **Nota** Si se selecciona un grupo de dispositivos diferente en la lista desplegable **Grupo de dispositivos**, únicamente se mostrarán los objetos de grupo de dispositivos (y objetos compartidos) creados para el grupo de dispositivos seleccionado.

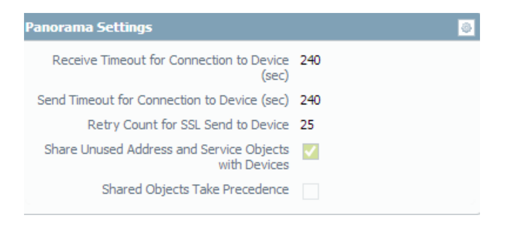
Gestión de objetos compartidos

Puede configurar el modo en que Panorama gestiona los objetos compartidos. Considere lo siguiente:

- Desea configurar Panorama únicamente para introducir en el dispositivo gestionado objetos compartidos a los que se hace referencia en políticas compartidas o políticas de grupo de dispositivos. Supongamos, por ejemplo, que todos los objetos de su implementación se han definido como objetos compartidos, pero que desea introducir únicamente los objetos relevantes para cada grupo de dispositivos. La casilla de verificación **Share Unused Address and Service Objects (Compartir objetos de direcciones y servicios no utilizados)** le permite limitar los objetos que se introducen en los dispositivos gestionados.

  De manera predeterminada, Panorama introduce todos los objetos compartidos (utilizados y no utilizados) en los dispositivos gestionados. En plataformas de bajo nivel, como PA-200, considere introducir únicamente los objetos compartidos relevantes en los dispositivos gestionados. Esto se debe a que el número de objetos que se puede almacenar en las plataformas de bajo nivel es considerablemente inferior al de las plataformas de medio y alto nivel. Asimismo, si tiene muchos objetos de direcciones y servicios no utilizados, al cancelar la selección de la casilla de verificación **Share Unused Address and Service Objects (Compartir objetos de direcciones y servicios no utilizados)** se reducen considerablemente los tiempos de compilación en los dispositivos debido a que la configuración introducida en cada dispositivo es menor.

  Sin embargo, al deshabilitar esta opción se puede aumentar el tiempo de compilación en Panorama. Esto se debe a que Panorama tiene que comprobar dinámicamente si se hace referencia a un objeto específico en una política.

OBJETOS COMPARTIDOS NO UTILIZADOS	
• Deshabilite el uso compartido de objetos de direcciones y servicios no utilizados con dispositivos. 	1. Seleccione **Panorama > Configuración > Gestión** y haga clic en el botón Editar en la sección Ajustes de Panorama. 2. Cancele la selección de la casilla de verificación **Compartir objetos de direcciones y servicios no utilizados con dispositivos**.

- Desea asegurarse de que un objeto compartido tiene prioridad sobre un objeto que tiene el mismo nombre que un objeto de grupo de dispositivos.

  De manera predeterminada, los objetos compartidos no cancelan ningún objeto de grupo de dispositivos con el mismo nombre que un objeto compartido.

Si desea evitar cancelaciones de objetos que se han definido como objetos compartidos en Panorama, puede habilitar la opción **Precedencia de objetos compartidos**. Cuando se habilita, todos los objetos de grupo de dispositivos con el mismo nombre se desecharán y los ajustes del objeto compartido se introducirán en los dispositivos gestionados.

PRECEDENCIA DE OBJETOS COMPARTIDOS	
• Asegúrese de que los objetos compartidos siempre tienen prioridad sobre los objetos de grupo de dispositivos.	1. Seleccione **Panorama > Configuración > Gestión** y haga clic en el botón Editar en la sección Ajustes de Panorama. 2. Seleccione la casilla de verificación **Precedencia de objetos compartidos**.

Dirección de políticas a un subconjunto de dispositivos

Dirigir políticas le permite especificar los dispositivos de un grupo de dispositivos en los que introducir las políticas. Le permite excluir uno o más dispositivos o sistemas virtuales, o bien únicamente aplicar la regla a dispositivos o sistemas virtuales específicos de un grupo de dispositivos.

La capacidad de dirigir una política le permite mantener las políticas centralizadas en Panorama; ofrece visibilidad y eficacia a la hora de gestionar las reglas. En lugar de crear reglas locales en un dispositivo o sistema virtual, las reglas de política dirigidas le permiten definir las reglas (como reglas compartidas o de grupo de dispositivos previas o posteriores) en Panorama.

DIRECCIÓN DE UNA POLÍTICA	
Paso 1. Cree una política.	1. Seleccione el **Grupo de dispositivos** para el que desea definir la política. 2. Seleccione la pestaña **Políticas** y seleccione la base de reglas para la que desea crear la política. Por ejemplo, defina una regla previa en la base de reglas de políticas de seguridad que permita a los usuarios de la red interna acceder a los servidores de DMZ: a. Haga clic en **Añadir** en **Políticas > Seguridad > Reglas previas**. b. Asigne a la regla un nombre descriptivo en la pestaña **General**. c. En la pestaña **Origen**, establezca **Zona de origen** como Fiable. d. En la pestaña **Destino**, establezca **Zona de destino** como DMZ. e. En la pestaña **Categoría de URL/servicio**, establezca **Servicio** como **predeterminado de aplicación**. f. En la pestaña **Acciones**, establezca **Configuración de acción** como **Permitir**. g. Deje el resto de opciones con los valores predeterminados.

DIRECCIÓN DE UNA POLÍTICA (CONTINUACIÓN)		
Paso 2	Dirija la política para incluir o excluir un subconjunto de dispositivos.	Para aplicar la política a un conjunto seleccionado de dispositivos: 1. Seleccione la pestaña **IP Destino** en la ventana Policy Rule (Regla de política). 2. Seleccione los dispositivos sobre los que desearía aplicar la regla. **Nota** De manera predeterminada, aunque la casilla de verificación de los sistemas virtuales en el grupo de dispositivos no esté seleccionada, todos los sistemas virtuales heredarán la regla al compilar. Seleccione la casilla de verificación de uno o más sistemas virtuales sobre los que desee aplicar la regla. 3. (Opcional) Para excluir un subconjunto de dispositivos para que no hereden la regla de política, seleccione la casilla de verificación **Instalar en todos los dispositivos menos los especificados**. 4. Haga clic en **ACEPTAR**. 5. Guarde los cambios de configuración. a. Haga clic en **Compilar** y seleccione **Panorama** como **Compilar tipo** para guardar los cambios en la configuración que se esté ejecutando. b. Haga clic en **Compilar** y seleccione **Grupo de dispositivos** como **Compilar tipo** para introducir los cambios en los dispositivos seleccionados en el grupo de dispositivos.

Visualización de jerarquía de reglas y búsqueda de reglas no utilizadas

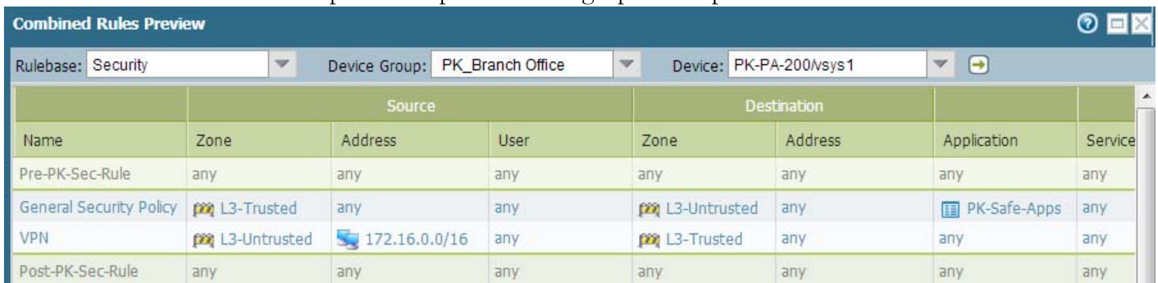
El orden de las reglas es esencial para proteger su red. Las reglas de política se evalúan de arriba a abajo. Un paquete coincide con la primera regla que cumpla los criterios definidos; después de activar una coincidencia, las reglas posteriores no se evalúan. Por lo tanto, las reglas más específicas deben preceder a las más genéricas para aplicar los mejores criterios de coincidencia.

Utilice el siguiente procedimiento para verificar el orden de las reglas y realizar los cambios adecuados:

VISTA PREVIA DE REGLAS Y VISUALIZACIÓN DE REGLAS NO UTILIZADAS

Paso 1. Visualice la jerarquía de reglas de cada base de reglas.

1. Seleccione la pestaña **Políticas** y haga clic en **Reglas de vista previa**.
2. Utilice los siguientes filtros para obtener una vista previa de las reglas:
   - **Fundamento de la regla**: Seleccione una base de reglas y visualice las reglas definidas para dicha base de reglas: seguridad, NAT, QoS, reenvío basado en políticas, descifrado, portal cautivo, cancelación de aplicación o protección DoS.
   - **Grupo de dispositivos**: Para la base de reglas seleccionada, puede ver todas las políticas con el estado **Compartido** o seleccionar un **Grupo de dispositivos** específico para el que desee ver la lista combinada de políticas heredadas de Panorama y las definidas localmente.
   - **Dispositivo**: Para la base de reglas y el grupo de dispositivos seleccionados, puede ver la lista de políticas que se evaluarán en un dispositivo específico en el grupo de dispositivos.



   Todas las reglas compartidas y de grupos de dispositivos heredadas de Panorama se muestran en verde y las reglas locales del dispositivo se muestran en azul; las reglas locales se incluyen entre las reglas previas y las posteriores.
3. Cierre la ventana Combined Rules (Reglas combinadas) para salir del modo de vista previa.

Paso 2 Busque reglas no utilizadas y, opcionalmente, elimine o deshabilite las reglas. Cada dispositivo mantiene una marca para las reglas que tienen una coincidencia. Panorama supervisa cada dispositivo, obtiene y agrega la lista de reglas sin coincidencia. Dado que la marca se restablece cuando se produce un restablecimiento del plano de datos al reiniciar, la práctica recomendada es supervisar esta lista periódicamente para determinar si la regla ha tenido una coincidencia desde la última comprobación antes de eliminarla o deshabilitarla.

1. Seleccione la pestaña **Políticas** y haga clic en **Resaltar reglas no utilizadas**.
   Las reglas no utilizadas actualmente se muestran con un fondo de puntos amarillos.
2. (Opcional) Para eliminar una regla no utilizada, seleccione la regla y haga clic en **Eliminar**.
3. (Opcional) Para deshabilitar una regla, seleccione la regla y haga clic en **Deshabilitar**. La regla deshabilitada aparece en cursiva.

VISTA PREVIA DE REGLAS Y VISUALIZACIÓN DE REGLAS NO UTILIZADAS (CONTINUACIÓN)	
Paso 3	Reordene las reglas dentro de una base de reglas de reglas previas o posteriores seleccionada, si es necesario. 1. En una base de reglas, seleccione la regla que desee mover. 2. Haga clic en las opciones **Mover hacia arriba**, **Mover hacia abajo**, **Mover a la parte superior** o **Mover a la parte inferior** para reordenar la colocación de la regla. **Nota** Para reordenar las reglas locales del dispositivo, cambie al contexto del dispositivo local.
Paso 4	Si modifica las reglas, guarde los cambios. 1. Haga clic en **Compilar** y seleccione **Panorama** como **Compilar tipo** para guardar los cambios en la configuración que se esté ejecutando. 2. Haga clic en **Compilar** y seleccione **Grupo de dispositivos** como **Compilar tipo** para introducir los cambios en los dispositivos seleccionados en el grupo de dispositivos.

Creación de plantillas

Las plantillas de Panorama le permiten gestionar las opciones de configuración en las pestañas **Dispositivo** y **Red** de los cortafuegos gestionados. Mediante las plantillas, puede definir una configuración básica para establecer centralmente las etapas de los nuevos cortafuegos y, a continuación, realizar excepciones específicas de dispositivos en la configuración, si es necesario. Por ejemplo, puede utilizar plantillas para definir el acceso administrativo al dispositivo, configurar ID de usuarios, gestionar certificados, establecer los cortafuegos en un clúster en alta disponibilidad y definir la configuración de logs y perfiles de servidor en los cortafuegos gestionados.

Al crear plantillas, asegúrese de asignar dispositivos parecidos a una plantilla. Por ejemplo, agrupe los dispositivos con un único sistema virtual en una plantilla y los dispositivos habilitados para varios sistemas virtuales en otra plantilla, o bien agrupe los dispositivos que necesiten una interfaz de red y una configuración de zona muy parecidas en una plantilla.

Consulte las siguientes secciones para obtener información sobre cómo trabajar con plantillas:

- Acciones para las que no se pueden utilizar las plantillas
- Adición de una nueva plantilla
- Cancelación de ajustes de plantilla
- Deshabilitación de ajustes de plantilla

Acciones para las que no se pueden utilizar las plantillas

Para los cortafuegos que ejecuten PAN-OS 4.x, el uso de plantillas de Panorama está limitado a lo siguiente:

- Creación de páginas de respuesta
- Definición de perfiles y secuencias de autenticación
- Creación de certificados autofirmados en Panorama o importación de certificados

- Creación de certificados de autenticación de clientes (conocidos como perfiles de certificado en Panorama 5.0 y posterior)
- Creación de perfiles de servidor: trap SNMP, Syslog, correo electrónico, flujo de red, RADIUS, LDAP y Kerberos

Para cortafuegos que ejecuten PAN-OS 5.x y posterior, las plantillas le permiten configurar una amplia gama de ajustes, con las siguientes excepciones:

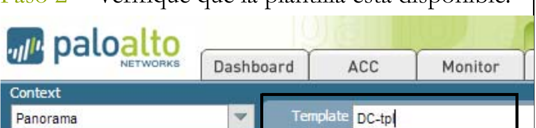
- No se pueden habilitar modos operativos como el modo de VSYS múltiple, el modo FIPS o el modo CC mediante plantillas; estos ajustes operativos deben configurarse localmente en cada dispositivo.
- No se puede configurar la información detallada de la dirección IP del clúster en HA del cortafuegos.

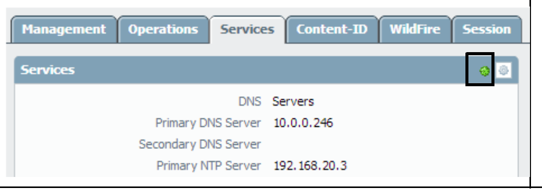
  La dirección IP del peer HA1, la dirección IP del peer de seguridad HA1, la dirección IP del peer HA2 y la dirección IP del peer de seguridad HA2 deben configurarse localmente en cada dispositivo gestionado.
- No se puede configurar una clave maestra y un diagnóstico.

Adición de una nueva plantilla

Las pestañas **Dispositivo** y **Red** necesarias para definir los elementos de configuración de red y los elementos de configuración de dispositivos en el cortafuegos no aparecerán hasta que no añada una plantilla en Panorama. Utilice estas instrucciones para añadir una nueva plantilla.

ADICIÓN DE UNA PLANTILLA	
Paso 1. Añada una nueva plantilla.	1. Seleccione **Panorama > Plantillas**. 2. Haga clic en **Añadir** e introduzca un nombre exclusivo y una descripción para identificar la plantilla. 3. (Opcional) Seleccione la casilla de verificación **Sistemas virtuales** si esta plantilla se utilizará para dispositivos con capacidad para VSYS múltiple que tengan habilitada la función VSYS múltiple. **Nota** Se producirá un fallo de compilación si se introduce una plantilla habilitada para dispositivos con capacidad para VSYS múltiple en dispositivos sin capacidad para VSYS múltiple o que no tengan habilitada la función VSYS múltiple. 4. Especifique el **Modo de operación** para los dispositivos a los que se aplicará la plantilla. El valor predeterminado es **normal**; cámbielo a **cc** o **fips**, si es necesario. La compilación de la plantilla fallará si no coincide el modo de operación especificado en la plantilla con lo que esté habilitado en los dispositivos incluidos en la plantilla. 5. (Opcional) Seleccione el **Modo de deshabilitación de VPN** al crear plantillas para modelos de hardware con el indicador -NV en el nombre del modelo; estos modelos están diseñados para no permitir una configuración de VPN en países que no permitan la conectividad de VPN. 6. Seleccione los **Devices (Dispositivos)** para los que piensa utilizar esta plantilla. Para aplicar una plantilla a un dispositivo, debe seleccionar los dispositivos individualmente. **Nota** Si se añade un nuevo dispositivo gestionado a Panorama, deberá añadir el nuevo dispositivo a la plantilla adecuada. Cuando compile sus cambios en la plantilla, la configuración se introducirá en todos los dispositivos asignados a la plantilla. 7. (Opcional) Seleccione la casilla de verificación **HA del peer de grupo** para cortafuegos que estén configurados como un clúster en HA. Añada ambos dispositivos o sistemas virtuales con la misma configuración a ambos peers. 8. Haga clic en **ACEPTAR**. 9. Haga clic en **Compilar** y seleccione **Panorama** como **Compilar tipo** para guardar los cambios en la configuración que se esté ejecutando. 10. Haga clic en **Compilar** y seleccione **Plantilla** como **Compilar tipo** para introducir los cambios en los dispositivos incluidos en la plantilla.

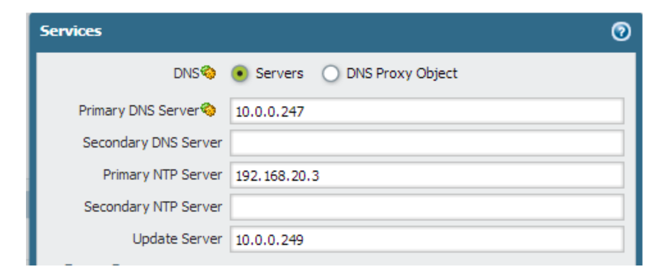
<table>
<tr><th colspan="2">ADICIÓN DE UNA PLANTILLA (CONTINUACIÓN)</th></tr>
<tr><td>Paso 2 Verifique que la plantilla está disponible.

</td><td>Después de añadir la primera plantilla, las pestañas Dispositivo y Red aparecerán en Panorama.
En las pestañas Red y Dispositivo, aparecerá la lista desplegable Plantilla. Verifique que la plantilla recién añadida aparece en la lista desplegable.</td></tr>
<tr><td>Paso 3 Aplique un cambio de configuración mediante la plantilla.

</td><td>Vamos a especificar una configuración básica que defina un servidor DNS principal para los dispositivos de la plantilla.
1. En la lista desplegable Plantilla, seleccione la plantilla que desee configurar.
2. Seleccione Dispositivo > Configuración > Servicios y edite la sección Servicios.
3. Introduzca una dirección IP para el Servidor DNS principal.
4. Haga clic en Compilar y seleccione Panorama como Compilar tipo para guardar los cambios en la configuración que se esté ejecutando.
5. Haga clic en Compilar y seleccione Plantilla como Compilar tipo para introducir los cambios en los dispositivos incluidos en la plantilla seleccionada.</td></tr>
<tr><td>Paso 4 Verifique que el dispositivo está configurado con los ajustes de plantilla que introdujo desde Panorama.

</td><td>1. Cambie al contexto de dispositivo para un cortafuegos en el que introdujo la configuración mediante la plantilla.
2. Vaya a Dispositivo > Configuración > Servicios. Aparecerá la dirección IP que introdujo mediante la plantilla. El icono de plantilla también aparecerá.</td></tr>
<tr><td colspan="2">Nota Para eliminar una plantilla, debe deshabilitar la plantilla en el dispositivo gestionado localmente. Debe tener privilegios de superusuario sobre el dispositivo para deshabilitar la plantilla.</td></tr>
</table>

Cancelación de ajustes de plantilla

Si bien las plantillas le permiten crear una configuración básica que puede aplicarse a varios dispositivos, puede que desee configurar ajustes específicos de dispositivo que no sean aplicables a todos los dispositivos de una plantilla. Las cancelaciones de plantillas permiten excepciones o modificaciones para cumplir sus necesidades de implementación. Si, por ejemplo, se utilizó una plantilla para crear una configuración básica pero varios dispositivos en un entorno de laboratorio de pruebas necesitan ajustes diferentes para la dirección IP del servidor DNS o el servidor NTP, puede cancelar la configuración definida en la plantilla.

CANCELACIÓN DE AJUSTES DE PLANTILLA	
Paso 1. Acceda a la interfaz web del dispositivo gestionado.	Puede iniciar directamente la dirección IP del cortafuegos o cambiar al contexto de dispositivo en Panorama.

CANCELACIÓN DE AJUSTES DE PLANTILLA (CONTINUACIÓN)	
Paso 2 Navegue hasta el ajuste que necesite modificar en el dispositivo. En este ejemplo, cancelaremos la dirección IP del servidor DNS que asignó mediante una plantilla en Creación de plantillas.	1. Vaya a **Dispositivo > Configuración > Servicios** y edite la sección Servicios. 2. Para cancelar la plantilla, haga clic en el icono para cancelar el valor definido para la dirección IP del servidor DNS principal. 3. Introduzca un nuevo valor para el servidor DNS principal. Tenga en cuenta que el icono de cancelación de plantilla se mostrará ahora para indicar que el valor que se introdujo mediante una plantilla se ha modificado en el dispositivo.  4. Haga clic en **ACEPTAR**. 5. Haga clic en **Compilar** para guardar sus cambios en el dispositivo.

Deshabilitación de ajustes de plantilla

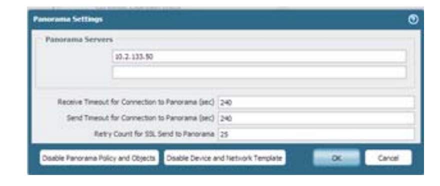
Si desea dejar de utilizar plantillas para gestionar la configuración de un dispositivo gestionado, puede deshabilitar la plantilla. Al deshabilitar una plantilla, puede decidir copiar los ajustes de plantilla en la configuración de dispositivo local o eliminar los valores que se introdujeron anteriormente mediante la plantilla.

CANCELACIÓN DE AJUSTES DE PLANTILLA	

1. Acceda a la interfaz web del dispositivo gestionado. Puede iniciar directamente la dirección IP del cortafuegos o cambiar al contexto de dispositivo en Panorama.

Nota Se requieren privilegios de superusuario para deshabilitar plantillas.

2. Seleccione **Dispositivo > Configuración > Gestión** y haga clic en el botón Editar en la sección Ajustes de Panorama.
3. Seleccione **Deshabilitar plantilla de dispositivo y red**.



4. (Opcional) Seleccione **Importar plantillas de dispositivos y red antes de deshabilitarlas** para guardar los ajustes de configuración localmente en el dispositivo. Si esta opción no está seleccionada, todos los ajustes introducidos por Panorama se eliminarán del dispositivo.
5. Haga clic en **ACEPTAR**.
6. Haga clic en **Compilar** para guardar los cambios.

Configuración de los cortafuegos para reenviar logs a Panorama

De forma predeterminada, todos los archivos de log se generan y almacenan localmente en el cortafuegos. Para agregar logs a Panorama, debe configurar cada cortafuegos para que reenvíe logs a Panorama.

Si tiene políticas de cumplimiento que requieren el archivado de datos, también puede reenviar logs a un servicio externo para el archivado, la notificación y/o el análisis. Panorama no puede reenviar logs recibidos desde los cortafuegos a un servidor externo.

Para establecer el reenvío de logs, realice las siguientes tareas:

- Cree un *perfil de servidor* para cada servicio externo al que desee que los cortafuegos reenvíen logs (Syslog, correo electrónico, trap SNMP) con destino de reenvío. Un perfil de servidor define cómo acceder al servidor remoto y autenticar para el servicio, si es necesario. No necesita un perfil de servidor si solamente tiene la intención de reenviar logs a Panorama o a un recopilador de logs.

- Configurar cada tipo de log para reenvío.

  Para cada tipo de log, puede especificar si se reenvía a Syslog, correo electrónico y/o receptor de traps SNMP, además de Panorama. Si tiene una arquitectura de recopilación de logs distribuida, al habilitar el reenvío a Panorama, la lista de preferencias de reenvío de logs se utiliza para reenviar logs a los recopiladores de logs configurados. Si bien puede realizar estas tareas manualmente en cada cortafuegos, puede utilizar grupos de dispositivos y plantillas en Panorama para lograr un flujo de trabajo más dinámico.

Tipo de log	Descripción	Flujo de trabajo con Panorama
Logs de tráfico	Para reenviar logs de tráfico, debe establecer un perfil de reenvío de logs y añadirlo a las políticas de seguridad en las que desee que se realice el reenvío. Únicamente se registra y reenvía el tráfico que coincida con una regla específica.	Utilice grupos de dispositivos para crear un perfil de reenvío de logs y reenviar logs de tráfico y amenaza [**Objects (Objetos) > Reenvío de logs**] a Panorama y a un servicio externo/servidor Syslog, si es necesario. Si está reenviando logs a un servicio externo/servidor Syslog, debe crear un perfil de servidor Syslog (**Dispositivo > Perfiles de servidor > Syslog**). El perfil de reenvío de logs utiliza el perfil de servidor Syslog, que configurará con plantillas, para acceder al servidor. Todos los logs de tráfico y amenaza reenviados a Panorama pueden visualizarse en la pestaña correspondiente en la pestaña **Supervisar > Logs**.
Logs de amenaza (incluye logs de filtrado de URL, WildFire y logs de filtrado de datos)	Para reenviar logs de amenaza, debe crear un perfil de reenvío de logs que especifique qué niveles de gravedad desea reenviar y, a continuación, añádalo a las políticas de seguridad en las que desee que se realice el reenvío. También debe adjuntar un perfil de seguridad (antivirus, antispyware, vulnerabilidad, filtrado de URL, bloqueo de archivos, filtrado de datos o protección DoS) a la política de seguridad. Una entrada de log de amenaza únicamente se creará (y se reenviará) si el tráfico asociado coincide con un perfil de seguridad. El resultado de los archivos analizados por WildFire se incluye con los logs de amenaza. Las entradas de log de WildFire con un veredicto benigno se registran como **Informativo**, mientras que las que tienen un veredicto de software malintencionado se registran como **Medio**. Por lo tanto, para habilitar el reenvío de logs a Panorama y a un servidor Syslog, debe habilitar eventos de niveles de gravedad informativo y medio.	

<table>
<tr><th>Tipo de log</th><th>Descripción</th><th>Flujo de trabajo con Panorama</th></tr>
<tr><td>Logs de sistema</td><td>Los logs de sistema muestran eventos del sistema, como fallos de HA, cambios de estado de enlaces y accesos administrativos al dispositivo. Para cada nivel de gravedad en el que desee reenviar logs, deberá seleccionar el reenvío a Panorama, correo electrónico, traps SNMP y un servidor Syslog, si es necesario.</td><td rowspan="3">Para logs Sistema, Configuración y Coincidencias HIP, debe configurar una plantilla y seleccionar la casilla de verificación Panorama para habilitar el reenvío a Panorama en la pestaña correspondiente en la pestaña Dispositivo > Configuración de log.

Para reenviar Syslogs a un servicio externo para el archivado en servidores Syslog tradicionales o en servidores SIEM (por ejemplo, Splunk, ArcSight, Qradar), también debe configurar un perfil de servidor mediante una plantilla (Dispositivo > Perfiles de servidor > Syslog).</td></tr>
<tr><td>Logs de configuración</td><td>Los logs de configuración registran cambios en la configuración. Para habilitar el reenvío de logs de configuración, deberá seleccionar el reenvío a Panorama, correo electrónico, traps SNMP y un servidor Syslog, si es necesario.</td></tr>
<tr><td>Logs de coincidencias HIP</td><td>Para habilitar el reenvío de logs de coincidencias HIP, deberá seleccionar el reenvío a Panorama, correo electrónico, traps SNMP y un servidor Syslog, si es necesario.

Los logs de coincidencias de perfil de información de host (HIP) se utilizan para compilar información sobre clientes de GlobalProtect. Se genera un log de coincidencias HIP cuando un dispositivo envía un informe HIP y un perfil HIP se configura con objetos HIP como versión del sistema operativo, nivel de parche, cifrado de disco, versión de antivirus, etc., que coincidan con el dispositivo.</td></tr>
</table>

Consulte la PAN-OS Getting Started Guide (Guía de inicio de PAN-OS) para obtener información detallada sobre cómo realizar estas tareas directamente en el cortafuegos.

Para obtener información sobre cómo reenviar los logs generados localmente por el propio Panorama, consulte Capítulo 6, Administración de Panorama.

CONFIGURACIÓN DEL REENVÍO DE LOGS	
Paso 1. (Opcional) Cree un perfil de servidor que contenga la información para conectarse al servicio externo/servidores Syslog.	1. Seleccione una plantilla o cree una nueva plantilla. Consulte el Paso 1 en Creación de plantillas. 2. Verifique que ha seleccionado una plantilla en la lista desplegable **Plantilla**. 3. Seleccione **Dispositivo > Perfiles de servidor > Syslog**. 4. Haga clic en **Añadir** y, a continuación, introduzca un **Nombre** para el perfil. 5. Haga clic en **Añadir** para añadir una nueva entrada del servidor Syslog e introduzca la información necesaria para conectar con el servidor Syslog (puede añadir hasta cuatro servidores Syslog al mismo perfil): • **Nombre**: Nombre exclusivo para el perfil de servidor. • **Servidor**: Dirección IP o nombre de dominio completo (FQDN) del servidor Syslog. • **Puerto**: El número de puerto por el que se enviarán mensajes de Syslog (el predeterminado es 514); debe especificar el mismo número de puerto en Panorama y en el servidor Syslog. • **Instalaciones**: Seleccione uno de los valores de Syslog estándar, que se usa para calcular el campo de prioridad (PRI) en la implementación de su servidor Syslog. Debe seleccionar el valor que asigna cómo usa el campo PRI para gestionar sus mensajes de Syslog. 6. (Opcional) Para personalizar el formato de los mensajes de Syslog que envía el cortafuegos, seleccione la pestaña **Formato de log personalizado**. Si desea más información sobre cómo crear formatos personalizados para los distintos tipos de log, consulte Common Event Format Configuration Guide (Guía de configuración de formato de eventos comunes). 7. Haga clic en **ACEPTAR** para guardar el perfil de servidor.

CONFIGURACIÓN DEL REENVÍO DE LOGS (CONTINUACIÓN)	
Paso 2 Configure un perfil de reenvío de logs para logs de tráfico y amenaza. **Nota** Los logs de amenaza incluyen filtrado de URL, filtrado de datos y logs de WildFire; los logs se reenvían basándose en los niveles de gravedad para los que habilite las notificaciones.	1. Cree un nuevo grupo de dispositivos o seleccione uno. Para crear un nuevo grupo de dispositivos, consulte Creación de grupos de dispositivos. 2. Seleccione **Objetos > Reenvío de logs**. 3. Haga clic en **Añadir** y, a continuación, introduzca un **Nombre** para el perfil de reenvío de logs. 4. (Opcional) Seleccione la casilla de verificación **Compartido** para aplicar estos ajustes a todos los dispositivos gestionados. 5. Seleccione la casilla de verificación **Panorama** para los niveles de gravedad en los que desee habilitar el reenvío de logs. 6. (Opcional) Seleccione el perfil de servidor para reenviar a un servidor Syslog. **Nota** Asegúrese de que el dispositivo (o sistema virtual) se incluye en el grupo de dispositivos y que la plantilla definida en el Paso 1 se aplica al dispositivo (o sistema virtual). 7. Haga clic en **ACEPTAR**.
Paso 3 Habilite el reenvío de logs para los logs Sistema, Configuración y Coincidencias HIP.	Con la misma plantilla seleccionada, opcionalmente, seleccione los tipos de logs que desee reenviar. • Para logs de sistema, seleccione **Dispositivo > Configuración de log > Sistema**, seleccione el enlace para cada **Gravedad**, habilite el reenvío a **Panorama** y seleccione el perfil de servidor que debe utilizarse para reenviar al servidor **Syslog**. • Para logs de configuración, seleccione **Dispositivo > Configuración de log > Configurar**, edite la sección Configuración de log > Configurar para habilitar el reenvío a **Panorama** y seleccione el perfil de servidor que debe utilizarse para reenviar al servidor **Syslog**. • Para logs de coincidencias HIP, seleccione **Dispositivo > Configuración de log > Coincidencia HIP**, edite la sección Configuración de log > Coincidencia HIP para habilitar el reenvío a **Panorama** y seleccione el perfil de servidor que debe utilizarse para reenviar al servidor **Syslog**.

CONFIGURACIÓN DEL REENVÍO DE LOGS (CONTINUACIÓN)		
Paso 4	(Opcional) Programe una exportación de logs a un servidor SCP o FTP. **Nota** Si tiene la intención de utilizar SCP, debe iniciar sesión en cada dispositivo gestionado y hacer clic en el botón **Conexión de servidor SCP de prueba** después de introducir la plantilla. La conexión no se establecerá mientras que el cortafuegos no acepte la clave de host para el servidor SCP.	Para logs de tráfico, amenaza, filtrado de URL, filtrado de datos y coincidencias HIP, puede programar una exportación de logs mediante plantillas de Panorama. 1. Seleccione la pestaña **Dispositivo > Programación de la exportación de logs**. 2. Seleccione la plantilla en la lista desplegable **Plantilla**. 3. Haga clic en **Añadir** y, a continuación, introduzca un **Nombre** para el perfil de reenvío de logs. 4. Seleccione la casilla de verificación **Habilitar** para habilitar la exportación de logs. 5. Seleccione el tipo de log que desee exportar. Para programar la exportación de más de un tipo de log, debe crear un perfil de exportación de logs para cada tipo de log. 6. Introduzca la hora del día (hh:mm) a la que comenzará la exportación en el formato de 24 horas (00:00 - 23:59). 7. Seleccione el protocolo que desea utilizar para exportar logs desde el cortafuegos a un host remoto. Puede utilizar **SCP** (seguro) o **FTP**. Para habilitar un FTP pasivo, seleccione la casilla de verificación **Habilitar modo pasivo de FTP**. 8. Defina la información detallada necesaria para conectarse al servidor. a. Introduzca el nombre de host o la dirección IP del servidor. b. Si es necesario para su servidor, introduzca el número de puerto (de manera predeterminada, FTP utiliza el puerto 21 y SCP utiliza el puerto 22), la ruta o el directorio en el que guardar los logs exportados y las credenciales de acceso (nombre de usuario y contraseña). 9. Haga clic en **ACEPTAR**.
Paso 5	Guarde todos los cambios de configuración.	1. Haga clic en **Compilar** y seleccione **Panorama** como **Compilar tipo** para guardar los cambios en la configuración que se esté ejecutando. 2. Haga clic en **Compilar** y seleccione **Plantilla** como **Compilar tipo** para introducir los cambios en los dispositivos incluidos en la plantilla seleccionada. 3. Haga clic en **Compilar** y seleccione **Grupos de dispositivos** como **Compilar tipo** para introducir los cambios en los dispositivos incluidos en el grupo de dispositivos seleccionado.

Compilación de cambios en Panorama

Cuando edita la configuración en Panorama, está haciendo cambios en el archivo de configuración candidata. La configuración candidata es una copia de la configuración que se está ejecutando junto con las modificaciones que ha guardado mediante la opción **Guardar**. La interfaz web de Panorama muestra todos los cambios de configuración inmediatamente; no obstante, los cambios no se implementarán hasta que no compile los cambios. El proceso de compilación valida los cambios en el archivo de configuración candidata y lo guarda como la configuración que se está ejecutando en Panorama.

Opciones de Panorama	Descripción
Panorama	Compila los cambios de la configuración candidata actual en la configuración que se está ejecutando en Panorama. Primero debe compilar sus cambios en Panorama, antes de compilar ninguna actualización de configuración (plantillas o grupos de dispositivos) en los dispositivos gestionados o grupos de recopiladores.
Plantilla	Compila los cambios de plantilla desde Panorama en los dispositivos seleccionados.
Grupo de dispositivos	Compila las políticas y los objetos configurados desde Panorama en los dispositivos/sistemas virtuales seleccionados.
Grupos de recopiladores	Compila los cambios en los grupos de recopiladores especificados gestionados por Panorama.

Al finalizar una compilación, se muestra un resultado. En una compilación realizada correctamente, aparece el mensaje **Compilaciones completadas**; si hay advertencias, aparece el mensaje **Compilación completada con advertencias**.

Algunas de las otras opciones que tiene al compilar los cambios son las siguientes:

- **Incluir plantillas de dispositivo y red**: Esta opción está disponible al compilar un grupo de dispositivos desde Panorama. Le permite compilar cambios de grupos de dispositivos y plantillas en los dispositivos pertinentes en una única operación de compilación.
  Si prefiere compilar sus cambios en operaciones de compilación separadas, no seleccione esta casilla de verificación.
- **Forzar valores de plantilla**: Al realizar una compilación de plantilla, la opción **Forzar valores de plantilla** cancela toda la configuración local y elimina los objetos de los dispositivos o sistemas virtuales seleccionados que no existan en la plantilla o hayan sido cancelados por la configuración local. Esta es una cancelación que revierte toda la configuración existente del dispositivo gestionado y garantiza que el dispositivo únicamente herede los ajustes definidos en la plantilla.
- **Combinar con configuración de candidato**: Cuando está habilitada, esta opción le permite combinar y compilar los cambios de configuración de Panorama con los cambios de configuración pendientes implementados localmente en el dispositivo de destino. Si esta opción no está habilitada, la configuración candidata del dispositivo no se incluye en la operación de compilación. Como práctica recomendada, deje esta opción deshabilitada si permite que los administradores de dispositivos modifiquen la configuración directamente en un dispositivo y no desea incluir sus cambios cuando compile cambios de Panorama. Otra práctica recomendada es utilizar la capacidad de auditoría de configuraciones de Panorama para revisar los cambios de configuración definidos localmente antes de emitir una compilación desde Panorama. Consulte Comparación de cambios en la configuración.

Modificación de los valores predeterminados de almacenamiento en búfer y reenvío de logs

Puede definir el modo de reenvío de logs que utilizan los cortafuegos para enviar logs a Panorama y, en el caso de una configuración de alta disponibilidad, especificar qué peer de Panorama puede recibir logs. Estas opciones están disponibles en la sección Logs e informes de la pestaña **Panorama > Configuración > Gestión**.

- Defina el modo de reenvío de logs en el dispositivo: The firewalls can forward logs to Panorama (pertains to both the M-100 appliance and the Panorama virtual appliance) in either *Buffered Log Forwarding* mode or in the *Live Mode Log Forwarding* mode.

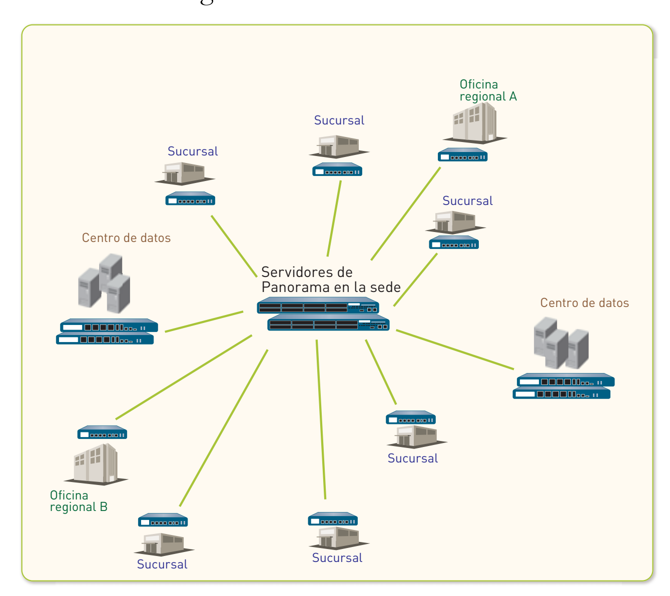
Opciones de creación de logs	Descripción
Reenvío de log en búfer desde dispositivo Valor predeterminado: Habilitado	Permite que cada dispositivo gestionado almacene logs en búfer y envíe los logs a intervalos de 30 segundos a Panorama (no configurable por el usuario). El reenvío de logs con almacenamiento en búfer es muy valioso cuando el dispositivo pierde la conexión con Panorama. El dispositivo almacena las entradas de log en búfer en su disco duro local y mantiene un puntero para registrar la última entrada de log enviada a Panorama. Cuando se restablece la conexión, el dispositivo reanuda el reenvío de logs desde donde lo dejó. El espacio en disco disponible para el almacenamiento en búfer depende de la cuota de almacenamiento de logs para la plataforma y el volumen de logs pendientes de sustitución. En el caso de que el dispositivo esté desconectado durante mucho tiempo y el último log reenviado se haya sustituido, todos los logs de su disco duro local se reenviarán a Panorama cuando vuelva a conectarse. Si se consume el espacio disponible del disco duro local del dispositivo, las entradas más antiguas se eliminarán para permitir el registro de nuevos eventos.
Live Mode Log Forwarding from Device (Reenvío de logs en modo en directo desde dispositivo) Esta opción está habilitada cuando se cancela la selección de la casilla de verificación **Reenvío de log en búfer desde dispositivo**.	En el modo en directo, el dispositivo gestionado envía cada transacción de log a Panorama al mismo tiempo que la registra en el dispositivo.

- Defina su preferencia de reenvío de logs en un dispositivo virtual de Panorama con una configuración de alta disponibilidad:
  - (cuando se registre en un disco virtual) habilite el registro únicamente en el disco local del peer de Panorama activo-primario. De manera predeterminada, ambos peers de Panorama con la configuración de HA reciben logs.
  - (cuando se registre en un NFS) habilite los dispositivos para que únicamente envíen los logs recién generados a un peer de Panorama secundario, que se promociona a principal, después de un fallo.

Opciones de creación de logs	Relativo a	Descripción
Solo logs principales activos al disco local Valor predeterminado: Deshabilitado	Dispositivo virtual de Panorama que se registra en un disco virtual y tiene una configuración de alta disponibilidad (HA).	Le permite configurar únicamente el peer de Panorama activo-primario para guardar logs en el disco local.
Obtener únicamente nuevos logs al convertir a principal Valor predeterminado: Deshabilitado	Dispositivo virtual de Panorama que se instala en un almacén de datos del sistema de archivos de red (NFS) y tiene una configuración de alta disponibilidad (HA).	Con el registro de NFS, cuando tiene un par de servidores de Panorama con una configuración de alta disponibilidad, solamente el peer de Panorama principal monta el almacén de datos de NFS. Por lo tanto, los dispositivos solamente pueden enviar logs al peer de Panorama principal, que puede escribir en el almacén de datos de NFS. Cuando se produce un fallo de HA, la opción **Obtener únicamente nuevos logs al convertir a principal** permite que un administrador configure los dispositivos gestionados únicamente envíen los logs recién generados a Panorama. Este evento se activa cuando la prioridad de Panorama activo-secundario se promociona a principal y puede empezar a registrar en NFS. Este comportamiento suele habilitarse para impedir que los dispositivos envíen grandes volúmenes de logs almacenados en búfer cuando se restablezca la conexión con Panorama después de un período de tiempo significativo.

Uso de Panorama para configurar dispositivos gestionados: ejemplo

Supongamos que desea utilizar Panorama con una configuración de alta disponibilidad para gestionar doce cortafuegos de su red: tiene seis cortafuegos implementados en seis sucursales, un par de cortafuegos con una configuración de alta disponibilidad en cada uno de los dos centros de datos y un cortafuegos en cada una de las dos oficinas centrales regionales.



Agrupación de dispositivos en grupos de dispositivos y plantillas

El primer paso para crear su estrategia de gestión central es determinar cómo agrupar los dispositivos en grupos de dispositivos y plantillas para introducir configuraciones de manera eficaz. Puede agrupar los dispositivos de diferentes formas basándose en la función empresarial del dispositivo, la ubicación geográfica o el dominio administrativo. En este ejemplo, creamos dos grupos de dispositivos y tres plantillas para administrar los dispositivos mediante Panorama.

Grupos de dispositivos

En este ejemplo, decidimos definir dos grupos de dispositivos basados en las funciones que realizarán los cortafuegos:

- *GD_SucursalYRegional* para agrupar dispositivos que sirvan de puertas de enlace de seguridad en las sucursales y las oficinas centrales regionales. Colocamos los cortafuegos de las sucursales y los cortafuegos de las oficinas regionales en el mismo grupo de dispositivos porque los dispositivos con funciones parecidas requerirán bases de reglas de políticas parecidas.
- *GD_CentroDeDatos* para agrupar los dispositivos que protegen los servidores en los centros de datos.

A continuación, podemos administrar las políticas compartidas entre ambos grupos de dispositivos y administrar las políticas de grupo de dispositivos distintas entre los grupos de oficinas regionales y sucursales. Para aumentar la flexibilidad, el administrador local de una oficina regional o sucursal puede crear reglas locales que coincidan con flujos de origen, destino y servicio específicos para acceder a aplicaciones y servicios necesarios para dicha oficina o sucursal. En este ejemplo, creamos la siguiente jerarquía para políticas de seguridad; puede utilizar un enfoque parecido para cualquiera de las otras bases de reglas:

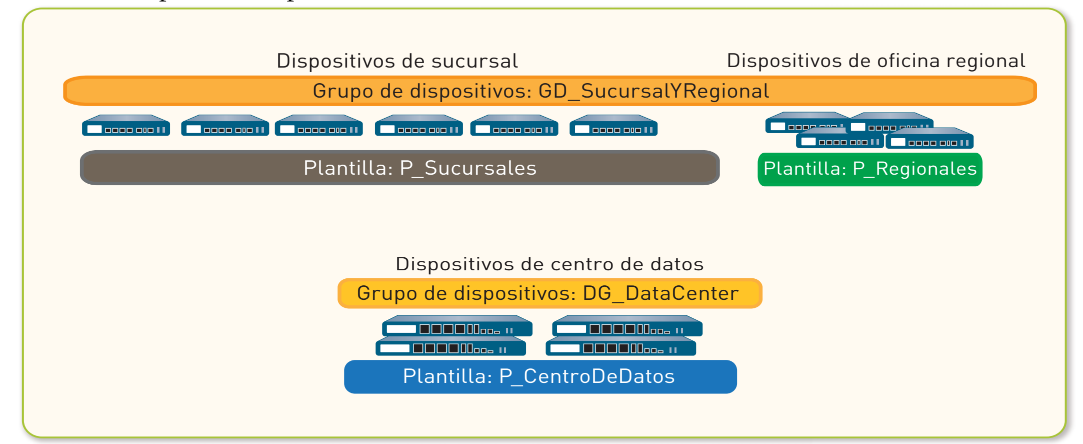
Grupos de dispositivos	GD_SucursalYRegional		GD_CentroDeDatos
Reglas	**Regional**	**Sucursal**	**Centro de datos**
Regla previa compartida	Permite servicios de DNS y SNMP.		
	Política de uso aceptable que niega el acceso a categorías de URL especificadas y tráfico punto a punto con un nivel de riesgo 3, 4 y 5.		
Regla previa de grupo de dispositivos	Permite conectarse a través de Facebook con todos los usuarios del grupo de marketing únicamente en las oficinas regionales.		Permite el acceso a la aplicación en la nube de Amazon para los hosts/servidores especificados del centro de datos.
Reglas locales de un dispositivo	Ninguna		
Regla posterior de grupo de dispositivos	Ninguna		
Regla posterior compartida	Para habilitar el registro de todo el tráfico de Internet en su red, cree una regla que permita o niegue todo el tráfico desde la zona fiable a la zona no fiable.		

Plantillas

Al agrupar dispositivos para plantillas, debemos tener en cuenta las diferencias en la configuración de red. Por ejemplo, los dispositivos deben incluirse en plantillas separadas si la configuración de interfaz no es la misma (las interfaces son distintas en cuanto a su tipo, las interfaces utilizadas no son iguales en el esquema de numeración y la capacidad de vinculación o las asignaciones de zona a interfaz son diferentes). Además, el modo en que se configuran los dispositivos para acceder a los recursos de red puede ser diferente debido a que los dispositivos están separados geográficamente; por ejemplo, el servidor DNS, los servidores Syslog y las puertas de enlace a los que acceden pueden ser diferentes. Por lo tanto, para lograr una configuración básica óptima, debe colocar los dispositivos en plantillas separadas, de la manera siguiente:

- *P_Sucursales* para los dispositivos de sucursales
- *P_Regionales* para los dispositivos de oficinas regionales

- *P_CentroDeDatos* para los dispositivos del centro de datos





Si tiene la intención de implementar sus cortafuegos en una configuración de HA activa/activa, asigne cada cortafuegos del clúster en HA a una plantilla separada. Al hacerlo logrará la flexibilidad necesaria para establecer configuraciones de red separadas para cada peer. Por ejemplo, puede gestionar las configuraciones de red en una plantilla separada para cada peer de modo que cada uno pueda conectarse a diferentes enrutadores hacia el norte y hacia el sur y pueda tener diferentes configuraciones de peer OSPF o BGP.

Planificación de sus políticas y configuración centralizadas

Utilicemos el ejemplo con el que empezamos arriba y realicemos las siguientes tareas para implementar y administrar centralmente los dispositivos gestionados:

Paso 1: Adición de dispositivos gestionados e implemente actualizaciones de contenido y actualizaciones de software PAN-OS en los dispositivos gestionados.

Paso 2: Utilice plantillas para administrar una configuración básica.

Paso 3: Utilice grupos de dispositivos para gestionar las políticas en sus cortafuegos.

Paso 4: Obtenga una vista previa de sus reglas y, a continuación, compile los cambios en Panorama, grupos de dispositivos y plantillas.

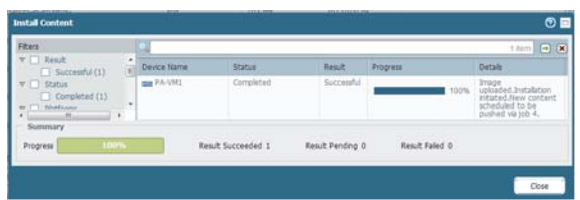
IMPLEMENTACIÓN DE ACTUALIZACIONES DE CONTENIDO Y ACTUALIZACIONES DE SOFTWARE PAN-OS EN LOS DISPOSITIVOS GESTIONADOS

Paso 1. Adición de dispositivos gestionados e implemente actualizaciones de contenido y actualizaciones de software PAN-OS en los dispositivos gestionados.

En primer lugar, instale la base de datos de **Aplicaciones** o **Aplicaciones y amenazas**, luego el **Antivirus** y, por último, actualice la versión de **Software**.

Si ha adquirido una suscripción a la prevención de amenazas, tendrá a su disposición las bases de datos de contenido y antivirus.

1. Seleccione **Panorama > Device Deployment (Implementación de dispositivos) > Actualizaciones dinámicas**.
   a. Haga clic en **Comprobar ahora** para comprobar las actualizaciones más recientes. Si el valor de la columna Acción es **Descargar** significa que hay una actualización disponible.
   b. Haga clic en **Descargar**. Cuando se complete la descarga, el valor en la columna Acción cambia a **Instalar**.
   c. Haga clic en el enlace **Instalar** de la columna **Acción**. Utilice los filtros o las pestañas definidas por el usuario para seleccionar los dispositivos gestionados en los que desee instalar esta actualización. Haga clic en **ACEPTAR**.
   d. Supervise el estado, el progreso y el resultado de la actualización de contenido de cada dispositivo. Podrá saber si la instalación se ha instalado correcta o incorrectamente en la columna **Results (Resultados)**.



Nota Para revisar el estado o el progreso de todas las tareas realizadas en Panorama, consulte Visualización del historial de finalización de tareas.

2. Seleccione **Panorama > Device Deployment (Implementación de dispositivos) > Software** para implementar actualizaciones de software.
   a. Haga clic en **Comprobar ahora** para comprobar las actualizaciones más recientes. Si el valor de la columna Acción es **Descargar** significa que hay una actualización disponible.
   b. Localice la versión que necesita para cada modelo de hardware y, a continuación, haga clic en **Descargar**. Cuando se complete la descarga, el valor en la columna Acción cambia a **Instalar**.
   c. Haga clic en el enlace **Instalar** de la columna Acción. Utilice los filtros o las pestañas definidas por el usuario para seleccionar los dispositivos gestionados en los que desee instalar esta versión.
   d. Habilite la casilla de verificación para **Upload only to device (do not install) [Actualizar únicamente en el dispositivo (no instalar)]** o **Reboot device after install (Reiniciar dispositivo después de instalar)** y haga clic en **ACEPTAR**. Podrá saber si la instalación se ha instalado correcta o incorrectamente en la columna **Results (Resultados)**.

USO DE PLANTILLAS PARA ADMINISTRAR UNA CONFIGURACIÓN BÁSICA
Paso 2 Utilice plantillas para administrar una configuración básica.
1. Cree plantillas y asigne los dispositivos adecuados a la plantilla. Consulte Añada una nueva plantilla.
2. Defina un servidor DNS, servidor NTP, servidor Syslog y titular de inicio de sesión. a. Seleccione la plantilla en la lista desplegable **Plantilla**. b. Seleccione **Dispositivo > Configuración > Servicios** y edite la sección Servicios. i Introduzca una dirección IP para el **Servidor DNS principal**. ii Introduzca una dirección IP para el **Servidor NTP principal**. c. Para añadir un servidor Syslog, seleccione **Dispositivo > Perfiles de servidor > Syslog**. i Introduzca un **Nombre** para el perfil. ii Haga clic en **Añadir** y, a continuación, haga clic en **Añadir** para añadir una nueva entrada del servidor Syslog e introduzca la información necesaria para conectar con el servidor Syslog (puede añadir hasta cuatro servidores Syslog al mismo perfil): • **Nombre**: Nombre exclusivo para el perfil de servidor. • **Servidor**: Dirección IP o nombre de dominio completo (FQDN) del servidor Syslog. • **Puerto**: El número de puerto por el que se enviarán mensajes de Syslog (el predeterminado es 514); debe utilizar el mismo número de puerto en Panorama y en el servidor Syslog. • **Instalaciones**: Seleccione uno de los valores de Syslog estándar, que se usa para calcular el campo de prioridad (PRI) en la implementación de su servidor Syslog. Debe seleccionar el valor que asigna cómo usa el campo PRI para gestionar sus mensajes de Syslog. iii Haga clic en **ACEPTAR** para guardar el perfil de servidor. d. Para añadir un titular de inicio de sesión, seleccione **Dispositivo > Configuración > Gestión** y edite la sección Configuración general. i Añada el texto del **Titular de inicio de sesión**. ii Haga clic en **ACEPTAR**. e. Repita las tareas de la 2a a la 2d para cada plantilla.
3. Habilite el acceso HTTPS, SSH y SNMP a la interfaz de gestión de los dispositivos gestionados. a. Seleccione la plantilla en la lista desplegable **Plantilla**. b. Seleccione **Dispositivo > Configuración > Gestión** y edite la sección Configuración de interfaz de gestión. c. Seleccione la casilla de verificación de **HTTPS**, **SSH** y **SNMP** bajo Servicios. d. Haga clic en **ACEPTAR**. e. Repita las tareas de la 3a a la 3d para cada plantilla.

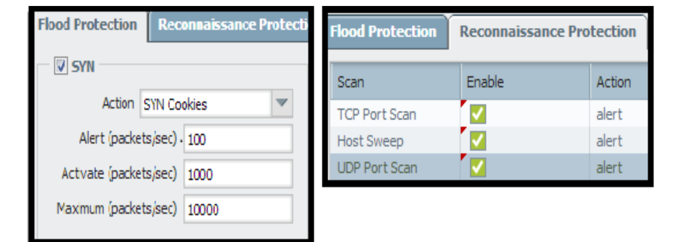
USO DE PLANTILLAS PARA ADMINISTRAR UNA CONFIGURACIÓN BÁSICA (CONTINUACIÓN)

4. Cree y adjunte un perfil de protección de zonas a la zona no fiable para los dispositivos de la plantilla del centro de datos (P_CentroDeDatos).

   a. Seleccione la plantilla en la lista desplegable **Plantilla**.

   b. Seleccione **Red > Perfiles de red > Protección de zonas**.

   c. Haga clic en **Añadir** para añadir un nuevo perfil e introduzca la información necesaria para definir el perfil. En este ejemplo habilitaremos la protección frente a una Inundación SYN y una alerta para Examen de puerto TCP, Limpieza de host y Examen de puerto de UDP.



   d. Para adjuntar el perfil a la zona no fiable, primero debe configurar la interfaz y los ajustes de zona en la plantilla.

Nota Debe haber configurado las interfaces en el dispositivo. Como mínimo, debe haber definido el tipo de interfaz, haberla asignado a un enrutador virtual, si es necesario, y haber adjuntado una zona de seguridad localmente en el dispositivo.

   i Seleccione **Red > Interface (Interfaz)**.

   ii Seleccione la interfaz adecuada en la tabla. Haga clic para configurar la interfaz.

   iii Seleccione el **Tipo de interfaz** en la lista desplegable.

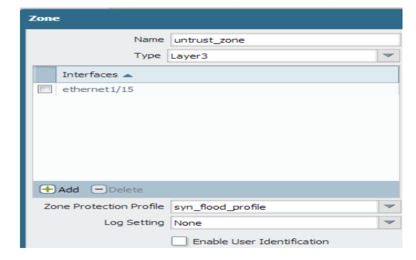
   iv Haga clic en el enlace **Enrutador virtual** en la lista desplegable **Nuevo Enrutador virtual** para crear un nuevo enrutador virtual. Asegúrese de que el nombre del enrutador virtual coincide con lo definido en el dispositivo.

   v Haga clic en el enlace **Nueva zona** en la lista desplegable **Zona de seguridad** para crear una nueva zona. Asegúrese de que el nombre de la zona coincide con lo definido en el dispositivo.

   vi Haga clic en **ACEPTAR**.

   vii Seleccione **Red > Zonas** y seleccione la zona que acaba de crear. Verifique que se ha adjuntado la interfaz correcta a la zona.

   viii En la lista desplegable **Perfil de protección de zona**, seleccione el perfil que creó arriba.



   ix Haga clic en **ACEPTAR**.

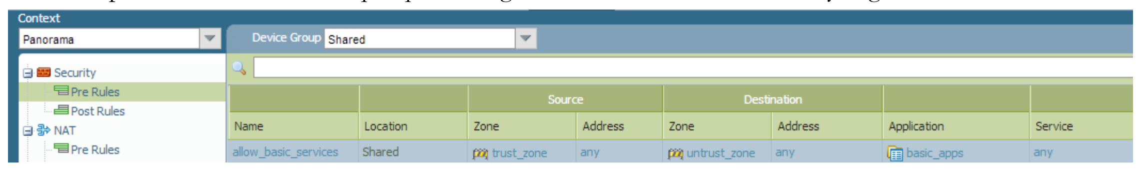
USO DE PLANTILLAS PARA ADMINISTRAR UNA CONFIGURACIÓN BÁSICA (CONTINUACIÓN)

5. Compile los cambios de plantilla.
   a. Haga clic en **Compilar** y seleccione **Panorama** como **Compilar tipo** para guardar los cambios en la configuración que se esté ejecutando. Haga clic en **ACEPTAR**.
   b. Haga clic en **Compilar** y seleccione **Plantilla** como **Compilar tipo** para introducir los cambios en los dispositivos incluidos en la plantilla seleccionada. Haga clic en **ACEPTAR**.

USO DE GRUPOS DE DISPOSITIVOS PARA INTRODUCIR POLÍTICAS

Paso 3 Utilice grupos de dispositivos para gestionar las políticas en sus cortafuegos.

1. Cree grupos de dispositivos y asigne los dispositivos adecuados a cada grupo de dispositivos. Consulte Cree grupos de dispositivos.
2. Cree una regla previa compartida para permitir servicios de DNS y SNMP.
   a. Cree un grupo de aplicaciones compartido para los servicios de DNS y SNMP.
      i Seleccione **Objects (Objetos) > Grupo de aplicaciones** y haga clic en **Añadir**.
      ii Introduzca un nombre y seleccione la casilla de verificación **Compartido** para crear un objeto del grupo de aplicaciones compartido.
      iii Haga clic en **Añadir**, escriba DNS y seleccione **dns** en la lista. Repita la operación para SNMP y seleccione **snmp**, **snmp-trap**.
      iv Haga clic en **ACEPTAR**. Se creará el grupo de aplicaciones para dns, snmp y snmp-trap.
   b. Cree la política compartida.
      i Seleccione el grupo de dispositivos **Compartido** en la lista desplegable **Grupo de dispositivos**.
      ii Seleccione la pestaña **Políticas** y seleccione **Reglas previas** en la base de reglas de políticas de **Seguridad**.
      iii Haga clic en **Añadir** e introduzca un **Nombre** para la regla de políticas de seguridad.
      iv En las pestañas **Origen** y **Destino** de la regla, haga clic en **Añadir** e introduzca una **Zona de origen** y una **Zona de destino** para el tráfico.
      v En la pestaña **Aplicaciones**, haga clic en **Añadir** y escriba el nombre del objeto del grupo de aplicaciones que definió antes; a continuación, selecciónelo en la lista desplegable.
      vi En la pestaña **Acciones**, verifique que Configuración de acción es **Permitir** y haga clic en **ACEPTAR**.



USO DE GRUPOS DE DISPOSITIVOS PARA INTRODUCIR POLÍTICAS (CONTINUACIÓN)

3. Defina la política de uso aceptable corporativa para todas las oficinas.

   En este ejemplo, crearemos una política compartida que restrinja el acceso a algunas categorías de URL y niegue el acceso al tráfico punto a punto con un nivel de riesgo 3, 4 y 5.

   a. Seleccione el grupo de dispositivos **Compartido** en la lista desplegable **Grupo de dispositivos**.

   b. Seleccione la pestaña **Políticas** y seleccione **Reglas previas** en la base de reglas de políticas de **Seguridad**.

   c. Haga clic en **Añadir** e introduzca un **Nombre** para la regla de políticas de seguridad.

   d. En las pestañas **Origen** y **Destino** de la regla, haga clic en **Añadir** y seleccione **Cualquiera** para **Zona de origen** y **Zona de destino** para el tráfico.

   e. Para definir el filtro de aplicación, en la pestaña **Aplicación**:

      i Haga clic en **Añadir** y haga clic en **Nuevo Filtro de aplicación**.

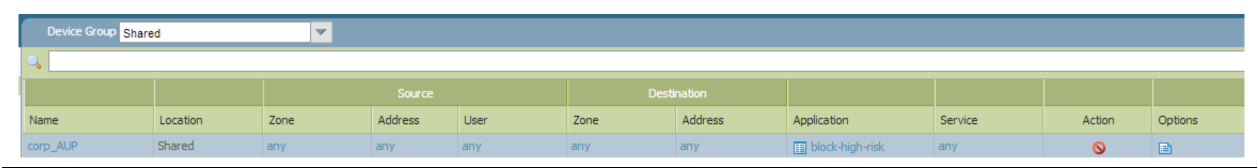
      ii Introduzca un **Nombre** y seleccione la casilla de verificación **Compartido**; en la sección Riesgo, seleccione los niveles **3**, **4** y **5**; y en la sección Tecnología, seleccione **punto a punto**.

      iii Haga clic en **ACEPTAR**.

   f. En la pestaña **Categoría de URL/servicio**, haga clic en **Añadir** y seleccione las categorías de URL que desearía bloquear, por ejemplo, archivos multimedia en secuencia, fechas y almacenamiento personal en línea.

   g. También puede adjuntar el perfil de filtrado de URL *predeterminado*, en la sección Ajuste de perfil de la pestaña **Acciones**.

   h. Haga clic en **ACEPTAR**.



4. Permite conectarse a través de Facebook con todos los usuarios del grupo de marketing únicamente en las oficinas regionales.

   Para habilitar una política de seguridad basada en usuarios y/o grupos, debe habilitar User-ID para cada zona que contenga usuarios que desee identificar. Debe haber configurado la identificación de usuarios en el cortafuegos [consulte la PAN-OS Getting Started Guide (Guía de inicio de PAN-OS)] y haber definido un dispositivo principal para el grupo de dispositivos. El dispositivo principal es el único dispositivo del grupo de dispositivos que recopila información de asignación de usuarios y grupos para la evaluación de políticas.

   a. Seleccione el grupo de dispositivos *GD_SucursalYRegional* en la lista desplegable **Grupo de dispositivos**.

   b. Seleccione la pestaña **Políticas** y seleccione **Reglas previas** en la base de reglas de políticas de **Seguridad**.

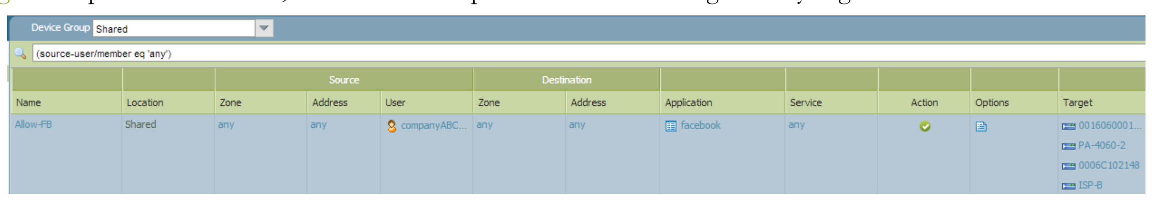
   c. Haga clic en **Añadir** e introduzca un **Nombre** para la regla de políticas de seguridad.

   d. En la pestaña **Usuario**, seleccione **Seleccionar**, haga clic en **Añadir** y seleccione el grupo de usuarios de marketing en la sección Usuario de origen.

   e. En la pestaña **Aplicación**, haga clic en **Añadir**, escriba *Facebook* y, a continuación, selecciónelo en la lista desplegable.

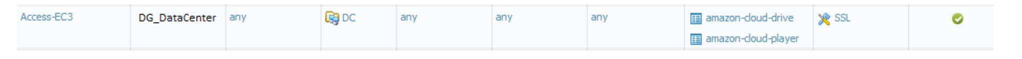
   f. En la pestaña **Acción**, verifique que la acción es **Permitir**.

   g. En la pestaña **IP Destino**, seleccione los dispositivos de oficinas regionales y haga clic en **ACEPTAR**.



USO DE GRUPOS DE DISPOSITIVOS PARA INTRODUCIR POLÍTICAS (CONTINUACIÓN)

5. Permite el acceso a la aplicación en la nube de Amazon para los hosts/servidores especificados del centro de datos.
   a. Cree un objeto de grupo de direcciones para los servidores/hosts del centro de datos que necesitan acceder a la aplicación en la nube de Amazon.
      i Seleccione **Objects (Objetos) > Grupos de direcciones**.
      ii Seleccione el grupo de dispositivos *GD_CentroDeDatos* en la lista desplegable **Grupo de dispositivos**.
      iii Haga clic en **Añadir** e introduzca un **Nombre** para el objeto de grupo de direcciones.
      iv Haga clic en **Añadir** y seleccione **Nueva dirección**.
      v Para definir el objeto de dirección, introduzca un **Nombre**, seleccione el **Tipo** y especifique una dirección IP de host, máscara de red IP, intervalo de IP o FQDN. Haga clic en **ACEPTAR**.
   b. Seleccione el grupo de dispositivos *GD_CentroDeDatos* en la lista desplegable **Grupo de dispositivos**.
      i Seleccione la pestaña **Políticas** y seleccione **Reglas previas** en la base de reglas de políticas de **Seguridad**.
      ii Haga clic en **Añadir** e introduzca un **Nombre** para la regla de políticas de seguridad.
      iii En la sección Dirección de origen de la pestaña **Origen**, haga clic en **Añadir** para seleccionar el grupo de direcciones que ha definido.
      iv En la pestaña **Aplicación**, haga clic en **Añadir**, escriba *amazon* y seleccione las aplicaciones de Amazon de la lista que se muestra.
      v En la pestaña **Acción**, verifique que la acción es **Permitir**.
      vi Haga clic en **ACEPTAR**.



6. Para habilitar el registro de todo el tráfico de Internet en su red, cree una regla que haga coincidir la zona fiable con la zona no fiable.
   a. Seleccione el grupo de dispositivos **Compartido** en la lista desplegable **Grupo de dispositivos**.
   b. Seleccione la pestaña **Políticas** y seleccione **Reglas previas** en la base de reglas de políticas de **Seguridad**.
   c. Haga clic en **Añadir** e introduzca un **Nombre** para la regla de políticas de seguridad.
   d. En las pestañas **Origen** y **Destino** de la regla, haga clic en **Añadir** y seleccione trust_zone (zona_fiable) como la zona de origen y untrust_zone (zona_no_fiable) como la zona de destino.
   e. En la pestaña **Acción**, verifique que la acción es **Denegar** y Ajuste de log es **Log al finalizar sesión**.
   f. Haga clic en **ACEPTAR**.

Paso 4 Obtenga una vista previa de sus reglas y, a continuación, compile los cambios en Panorama, grupos de dispositivos y plantillas.

1. Seleccione la pestaña **Políticas** y haga clic en **Reglas de vista previa**. Esta vista previa le permite evaluar visualmente de qué modo se organizan sus reglas por capas para una base de reglas específica.
2. Haga clic en **Compilar** y seleccione Compilar tipo como **Panorama**. Haga clic en **ACEPTAR**.
3. Haga clic en **Compilar** y seleccione Compilar tipo como **Grupos de dispositivos**. Verifique que la opción **Incluir plantillas de dispositivo y red** está habilitada. Haga clic en **ACEPTAR**.
4. Cambie al contexto de dispositivo para iniciar la interfaz web de un dispositivo gestionado y confirme que se han aplicado las configuraciones de plantillas y políticas.

Habilitación de logs

Todos los cortafuegos de nueva generación de Palo Alto Networks pueden generar logs que ofrecen un seguimiento auditado de las actividades y eventos del cortafuegos. Para supervisar centralmente los logs y generar informes, debe reenviar los logs generados en los cortafuegos gestionados a Panorama. Si está implementando un dispositivo virtual de Panorama con un disco virtual o se está registrando en un NFS, no necesita realizar ninguna tarea adicional para habilitar los logs.

Si va a registrarse en un dispositivo M-100 (ya sea localmente en un M-100 en modo Panorama, o en un recopilador de logs específico gestionado por un dispositivo virtual de Panorama o un dispositivo M-100 en modo Panorama), debe realizar ciertas tareas adicionales para habilitar la recopilación de logs.

Debe añadir cada recopilador de logs como recopilador gestionado y crear grupos de recopiladores para acceder, gestionar y actualizar los recopiladores de logs mediante Panorama. Después de añadir y configurar los recopiladores de logs en Panorama, Panorama introduce la configuración necesaria en los dispositivos gestionados. No necesita configurar explícitamente los dispositivos gestionados para reenviar logs a un recopilador de logs.

Realice las tareas siguientes para habilitar los logs:

▲ Adición de un recopilador de logs a Panorama

▲ Configuración de grupos de recopiladores

▲ Verificación de la habilitación del reenvío de logs

▲ (Opcional) Modificación de los valores predeterminados de almacenamiento en búfer y reenvío de logs

Adición de un recopilador de logs a Panorama

Para que Panorama (dispositivo virtual de Panorama o dispositivo M-100 en modo Panorama) gestione un recopilador de logs, debe añadir el recopilador de logs como recopilador gestionado. Si el dispositivo M-100 no está ya configurado en modo de recopilación de logs, consulte Configuración del dispositivo M-100 en modo de recopilación de logs.

Si está utilizando un dispositivo M-100 en modo Panorama, el recopilador de logs *predeterminado* local en Panorama se añade durante el proceso de fabricación. Sin embargo, si ha cargado/migrado la configuración desde un dispositivo virtual de Panorama al dispositivo M-100, el recopilador de logs predeterminado no aparecerá; utilice las instrucciones de esta sección para añadir el recopilador de logs y, a continuación, Configuración de grupos de recopiladores.

ADICIÓN DE UN RECOPILADOR GESTIONADO		
Paso 1.	Añada un recopilador gestionado.	1. Seleccione **Panorama > Recopiladores gestionados**. 2. Seleccione **Añadir**.
Paso 2	Añada el número de serie del recopilador de logs en Panorama.	1. En la pestaña **General**, introduzca el número de serie del recopilador de logs en el campo **Nº serie recopilador**. • Si el recopilador de logs es local en Panorama, introduzca el número de serie que aparece en el **Panel**. • Si va a añadir un recopilador de logs específico, introduzca el número de serie de ese dispositivo M-100.

ADICIÓN DE UN RECOPILADOR GESTIONADO (CONTINUACIÓN)

Paso 3 Realice estas tareas únicamente si va a añadir un recopilador de logs específico.

Como el recopilador de logs predeterminado se encuentra en el mismo dispositivo físico que Panorama que lo está gestionando, no necesita configurar las preferencias de autenticación o acceso de gestión para él.

Nota Un dispositivo M-100 en modo de recopilación de logs únicamente tiene acceso a la CLI; no hay ninguna interfaz web para gestionar un recopilador de logs.

1. Configure los ajustes de acceso de red.

   Aunque ya ha especificado esta información detallada durante la configuración inicial en el recopilador de logs, debe volver a introducir la información en la pestaña **Panorama > Recopiladores gestionados**.

   a. En la pestaña **General**, añada la dirección IP de los servidores de Panorama que gestionarán el recopilador de logs. Si ha implementado Panorama en HA, añada la dirección IP para los peers principal y secundario.

   b. Configure las direcciones IP del servidor DNS.

   c. (Opcional) Establezca la zona horaria que se utilizará para registrar las entradas de log.

2. Mediante Panorama, configure el acceso administrativo para el recopilador de logs.

   a. En la pestaña **Autenticación**, el usuario predeterminado es **admin**. No puede modificar este nombre de usuario ni añadir usuarios administrativos al recopilador de logs.

   b. Especifique el número de **Intentos fallidos** al iniciar sesión tras los que el usuario se bloqueará y no podrá acceder al recopilador de logs, así como el intervalo de tiempo durante el cual el usuario estará bloqueado en **Tiempo de bloqueo**.

   c. Especifique una contraseña. Para generar una contraseña con hash, realice las siguientes tareas:

      i Introduzca el siguiente comando en la CLI:

      ```
      request password-hash password <sucontraseña>
      ```

      La CLI mostrará el resultado con hash para la contraseña que introduzca.

      ii Copie el valor con hash y péguelo en el campo **Hash de la contraseña**.

      Cuando compile los cambios en el grupo de recopiladores, la nueva contraseña con hash se introducirá en el recopilador de logs.

3. Especifique los ajustes del puerto de gestión (MGT) que definió en el recopilador de logs durante la configuración inicial.

   a. En la pestaña **Gestión**, introduzca la **Dirección IP**, **Máscara de red** y dirección IP de **Puerta de enlace predeterminada** definidas en el recopilador de logs.

   b. (Opcional) Habilite el acceso **SNMP** para supervisar el recopilador de logs. De manera predeterminada, tiene SSH y ping habilitados en el puerto de gestión.

   c. (Opcional) Para restringir el acceso al recopilador de logs, haga clic en **Añadir** e introduzca una o más direcciones IP en la lista **Direcciones IP permitidas**.

   Nota Como únicamente las direcciones IP especificadas pueden acceder al recopilador de logs, asegúrese de añadir la dirección IP de los dispositivos que necesiten conectarse y reenviar logs al recopilador de logs.

   d. Haga clic en **ACEPTAR**.

ADICIÓN DE UN RECOPILADOR GESTIONADO (CONTINUACIÓN)		
Paso 4	Guarde los cambios.	Haga clic en **Compilar** y, en Compilar tipo, seleccione **Panorama**. Haga clic en **ACEPTAR**.
Paso 5	Verifique que el recopilador de logs se ha añadido y está conectado a Panorama.	Seleccione **Panorama > Recopiladores gestionados** y compruebe que se muestra el recopilador gestionado que ha añadido.
Paso 6	Habilite los pares de discos para los logs. Para configurar los discos en un par de RAID, consulte Aumento de la capacidad de almacenamiento en el dispositivo M-100.	De manera predeterminada, el par de discos A tiene habilitado RAID y se ha añadido al recopilador de logs. Si ha añadido más pares de RAID para aumentar la capacidad de almacenamiento: 1. Haga clic en **Añadir** en la pestaña **Discos**. 2. Seleccione cada par de discos adicional en la lista desplegable. 3. Haga clic en **ACEPTAR** para hacer que el nuevo par de discos esté disponible para los logs. 4. Haga clic en **Compilar** y, en Compilar tipo, seleccione **Panorama**. Haga clic en **ACEPTAR**.
Paso 7	Verifique que los discos están habilitados, disponibles y presentes.	Seleccione **Panorama > Recopiladores gestionados** y haga clic en el enlace **Estadísticas**. La ventana Collector Statistics (Estadísticas del recopilador) mostrará el estado de los pares de discos que ha añadido.

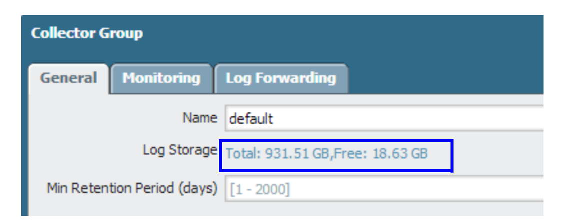
Configuración de grupos de recopiladores

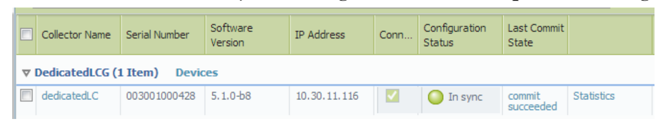
Después de añadir un recopilador de logs como recopilador gestionado, debe asignarlo a un grupo de recopiladores para que pueda gestionarse y configurarse con Panorama. Un grupo de recopiladores le permite asignar los cortafuegos gestionados a los recopiladores de logs del grupo de recopiladores.

Aunque un grupo de recopiladores puede incluir uno o más recopiladores de logs, Palo Alto Networks recomienda colocar únicamente un recopilador de logs en un grupo de recopiladores. Sin embargo, si requiere más de 4 TB de capacidad de almacenamiento de logs, deberá añadir varios recopiladores de logs a un grupo de recopiladores. Para comprender cómo funcionan los logs con varios recopiladores de logs en un grupo de recopiladores, consulte Uso de varios recopiladores de logs en un grupo de recopiladores.

Si está utilizando un dispositivo M-100 en modo Panorama, se le configurará un grupo de recopiladores predeterminado que contenga el recopilador de logs predeterminado. Utilice las instrucciones de esta sección para configurar el grupo de recopiladores predeterminado. Si está utilizando un recopilador de logs específico, primero debe Adición de un recopilador de logs a Panorama y utilizar las instrucciones de esta sección para crear un grupo de recopiladores.

CONFIGURACIÓN DE GRUPOS DE RECOPILADORES		
Paso 1.	Añada un grupo de recopiladores.	1. Seleccione **Panorama > Grupos de recopiladores**. Existe un grupo de recopiladores **predeterminado** para un dispositivo M-100 en modo Panorama. 2. Seleccione el enlace del grupo de recopiladores **predeterminado** para modificarlo o haga clic en **Añadir** para definir un nuevo grupo de recopiladores.
Paso 2	Defina los miembros del grupo de recopiladores.	1. Seleccione la pestaña **Reenvío de logs** en la ventana Grupo de recopiladores. 2. Haga clic en **Añadir** en la sección Collector Group Members (Miembros del grupo de recopiladores) y seleccione los recopiladores de logs que desea incluir en el grupo de recopiladores. Únicamente los recopiladores de logs que haya añadido como recopiladores gestionados se mostrarán en la lista de selección.
Paso 3	Seleccione qué dispositivos pueden reenviar logs a este grupo de recopiladores. **Nota** Si su red tiene cortafuegos que ejecuten PAN-OS versión 4.x y 5.x, puede asignar los cortafuegos que ejecuten PAN-OS v5.x para reenviar logs a un recopilador de logs específico. Los cortafuegos que ejecuten PAN-OS v4.x no pueden asignarse a un recopilador de logs; deben enviar los logs a un dispositivo virtual de Panorama o un dispositivo M-100 en modo Panorama.	1. En la pestaña **Reenvío de logs** de la ventana Grupo de recopiladores, haga clic en **Añadir** en la sección Log Forwarding Preferences (Preferencias de reenvío de logs). 2. Haga clic en **Modify (Modificar)**, seleccione el **Dispositivo** gestionado en las opciones de visualización filtradas y haga clic en **ACEPTAR**. A continuación, haga clic en **Añadir** en la sección Recopiladores y seleccione el recopilador de logs. Los dispositivos seleccionados pueden enviar logs al recopilador de logs asignado en el grupo de recopiladores. Log Forwarding Preferences Device / Collectors PA-4060-1 / CandleStick **Nota** Si tiene varios recopiladores de logs en el grupo de recopiladores, haga clic en **Añadir** de nuevo y seleccione otro recopilador de logs para definir una lista con prioridades. El primer recopilador de logs de la lista es el recopilador de logs principal asignado al cortafuegos. 3. Haga clic en **ACEPTAR**.

CONFIGURACIÓN DE GRUPOS DE RECOPILADORES (CONTINUACIÓN)	
Paso 4 Asigne el porcentaje de capacidad de almacenamiento para cada tipo de log. Si la capacidad de almacenamiento de logs aparece como 0 MB, puede que no haya añadido los recopiladores de logs al grupo de recopiladores. Complete el Paso 2 y, a continuación, vuelva a esta tarea (Paso 4). Si sigue indicando 0 MB, compruebe que ha habilitado los pares de discos y ha compilado los cambios en el grupo de recopiladores. Consulte el Paso 6 en la sección Adición de un recopilador de logs a Panorama.	1. Seleccione la pestaña **General** en la ventana Grupo de recopiladores**.** 2. Haga clic en el enlace que muestra la capacidad **Almacenamiento de log** del grupo de recopiladores.  3. Modifique la **cuota** asignada a cada tipo de log. Conforme cambia los valores, la pantalla se actualiza para mostrar el valor del número correspondiente (GB/MB) para el porcentaje asignado basado en el porcentaje total en el grupo de recopiladores. 4. (Opcional) Haga clic en **Restablecer valores predeterminados** si necesita deshacer los cambios y restablecer las cuotas a los valores predeterminados de fábrica.
Paso 5 Defina el tiempo mínimo de retención de logs del grupo de recopiladores. El tiempo mínimo de retención de logs informa a Panorama cuándo generar una alerta si la capacidad de almacenamiento se acerca a su capacidad completa.	1. Seleccione la pestaña **General** en la ventana Grupo de recopiladores**.** 2. Introduzca un valor entre 1-2.000 días para el **Minimum Retention Period (Periodo mínimo de retención)**. Este valor especifica cuánto tiempo desea conservar los logs. Se genera un log de sistema en Panorama cuando la fecha actual menos la fecha de log más antigua es un valor inferior al periodo mínimo de retención definido.

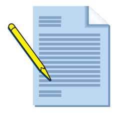
CONFIGURACIÓN DE GRUPOS DE RECOPILADORES (CONTINUACIÓN)	
Paso 6 (Opcional) Configure la supervisión de SNMP para el grupo de recopiladores. Puede utilizar SNMP para recopilar la siguiente información en el grupo de recopiladores: estado de conexión, estadísticas de unidad de disco, versión de software, CPU media, media de logs/segundo y duración de almacenamiento de logs para cada tipo de log. **Nota** Para permitir que el gestor de SNMP interprete la información, debe cargar los archivos MIB de PAN-OS en su software de gestión de SNMP y, si es necesario, compilarlos. A continuación, debe configurar el software de gestión de SNMP para que supervise los OID que le interesan.	1. Seleccione la pestaña **Supervisando** en la ventana Grupo de recopiladores. 2. Introduzca una cadena de texto para especificar la **Ubicación** física del grupo de recopiladores de logs. 3. Añada la dirección de correo electrónico de un **contacto** administrativo. 4. Seleccione la **versión** SNMP y, a continuación, introduzca los detalles de configuración de la siguiente forma (según la versión SNMP que utilice) y, a continuación, haga clic en **ACEPTAR**: • **V2c**: introduzca la **cadena de comunidad SNMP** que permita al gestor de SNMP acceder al agente de SNMP del grupo de recopiladores. El valor predeterminado es **público**. Sin embargo, como se trata de una cadena de comunidad ampliamente conocida, la práctica recomendada es usar un valor que no se adivine fácilmente. • **V3**: debe crear al menos una vista y un usuario para poder utilizar SNMPv3. La vista especifica a qué información de gestión tiene acceso el gestor. Si desea permitir el acceso a toda la información de gestión, solo tiene que introducir el OID de nivel más alto de .1.3.6.1 y especificar la **opción** como **incluir** (también puede crear vistas que excluyan determinados objetos). Utilice **0xf0** como la **máscara**. A continuación, cuando cree un usuario, seleccione la **vista** que acaba de crear y especifique la **contraseña de autenticación** y la **contraseña privada**. La configuración de autenticación (la cadena de comunidad para V2c o el nombre de usuario y las contraseñas para V3) establecida en el grupo de recopiladores debe coincidir con el valor configurado en el gestor de SNMP. 5. Haga clic en **ACEPTAR** para guardar estos ajustes.
Paso 7 Guarde los cambios.	1. Haga clic en **Compilar** y, en Compilar tipo, seleccione **Panorama**. Haga clic en **ACEPTAR**. 2. Haga clic en **Compilar** y, en Compilar tipo, seleccione **Grupo de recopiladores**. Haga clic en **ACEPTAR**.
Paso 8 Verifique que el recopilador de logs está conectado y sincronizado con Panorama.	1. Seleccione **Panorama > Recopiladores gestionados** y verifique el estado de conexión y de configuración del recopilador de logs. 

Eliminación de un dispositivo de un grupo de recopiladores

En una implementación de recopilación de logs distribuida en la que tenga recopiladores de logs específicos, si necesita que un dispositivo envíe logs a Panorama en lugar de enviar logs al grupo de recopiladores, debe eliminar el dispositivo del grupo de recopiladores.

Al eliminar el dispositivo del grupo de recopiladores y compilar el cambio, el dispositivo enviará los logs automáticamente a Panorama en lugar de enviarlos a un recopilador de logs.

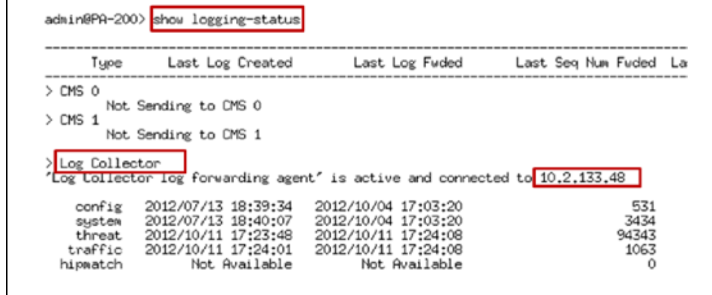
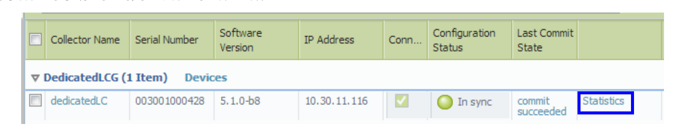
ELIMINACIÓN DE UN DISPOSITIVO DE UN GRUPO DE RECOPILADORES
1. Seleccione la pestaña **Panorama > Grupos de recopiladores**.
2. Haga clic en el enlace del grupo de recopiladores que desee y seleccione la pestaña **Reenvío de logs**.
3. En la sección Log Forwarding Preferences (Preferencias de reenvío de logs), seleccione el dispositivo que desee eliminar de la lista y haga clic en **Eliminar**.
4. Haga clic en **ACEPTAR**.
5. Haga clic en **Compilar** y, en Compilar tipo, seleccione **Panorama**. Haga clic en **ACEPTAR**.
6. Haga clic en **Compilar** y, en Compilar tipo, seleccione **Grupo de recopiladores**. Haga clic en **ACEPTAR**.



Para eliminar temporalmente la lista de preferencias de reenvío de logs del dispositivo, puede eliminarla con la CLI en el dispositivo. Sin embargo, debe eliminar los cortafuegos asignados en la configuración del grupo de recopiladores de Panorama. De lo contrario, la próxima vez que compile cambios en el grupo de recopiladores, el dispositivo volverá a configurarse para enviar logs al recopilador de logs asignado.

Verificación de la habilitación del reenvío de logs

Ahora que ha añadido los recopiladores de logs como recopiladores gestionados, ha creado y configurado el grupo de recopiladores y ha asignado los dispositivos gestionados para reenviar logs al grupo de recopiladores especificado, puede comprobar que la configuración se ha realizado correctamente.

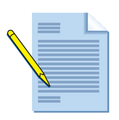
VERIFICACIÓN DEL REENVÍO DE LOGS	
Paso 1. En el dispositivo gestionado, compruebe que el dispositivo tiene la lista de preferencias de reenvío de logs y está reenviando los logs al recopilador de logs configurado. No puede ver esta información desde la interfaz web del dispositivo.	1. Acceda a la CLI en el dispositivo. 2. Introduzca los siguientes comandos: a. **`show log-collector preference-list`** Si ha asignado únicamente un recopilador de logs al grupo de recopiladores, la pantalla resultante se parecerá a esta: `Log collector Preference List` `Serial Number: 003001000024` `IP Address:10.2.133.48` b. **`show logging-status`** La pantalla resultante se parecerá a esta: 
Paso 2 En Panorama, verifique la tasa de recopilación de logs.	Haga clic en el enlace **Estadísticas** de la pestaña **Panorama > Recopiladores gestionados** para ver la media de logs/segundo que está recibiendo Panorama. 

Implementación de actualizaciones de software y gestión de licencias

Como administrador, puede utilizar Panorama para realizar un seguimiento y gestionar licencias de manera central y gestionar actualizaciones de software y actualizaciones de contenido dinámico en los dispositivos gestionados y los recopiladores gestionados. Panorama hace una comprobación con el servidor de licencias o servidor de actualización de Palo Alto Networks, verifica la validez de la solicitud y, a continuación, permite la recuperación e instalación de la licencia/versión de software en el dispositivo gestionado o recopilador de logs. Esta capacidad facilita la implementación, ya que no necesita realizar las tareas repetitivamente en cada dispositivo/recopilador de logs. Es de especial utilidad para dispositivos gestionados que no tienen un acceso directo a Internet o para gestionar actualizaciones del dispositivo M-100 configurado en modo de recopilación de logs, que no admite una interfaz web.

Utilice esta capacidad de implementación centralizada para admitir nuevas actualizaciones de contenido o actualizaciones de software en dispositivos seleccionados antes de realizar la actualización en todos los dispositivos gestionados. También puede recuperar nuevas licencias con un código de autorización e introducir las claves de licencia en el dispositivo gestionado.

Dependiendo de qué suscripciones estén activas en cada dispositivo, las actualizaciones de contenido pueden incluir la actualización de aplicación/actualizaciones de firma de aplicación y amenaza más recientes, firmas de antivirus, actualizaciones de WildFire y actualizaciones de archivos de datos de GlobalProtect. Las actualizaciones de software que puede gestionar desde Panorama incluyen: PAN-OS, cliente SSL VPN y cliente de GlobalProtect.



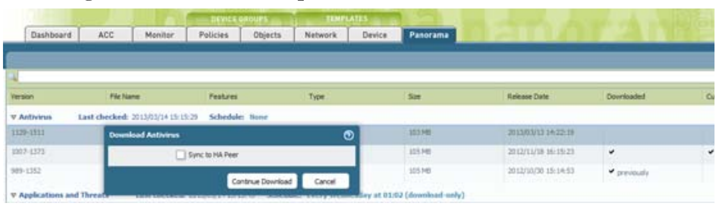
Debe activar la suscripción a la asistencia técnica directamente desde cada cortafuegos; no se puede utilizar Panorama para implementar la suscripción a la asistencia técnica.

<table>
<tr><th colspan="2">IMPLEMENTACIÓN DE SOFTWARE Y LICENCIAS EN DISPOSITIVOS GESTIONADOS MEDIANTE PANORAMA</th></tr>
<tr><td>

• Implemente actualizaciones dinámicas.

Basándose en las suscripciones que haya adquirido, puede que necesite instalar actualizaciones de **Antivirus**, actualizaciones de **Applications (Aplicaciones)** o **Aplicaciones y amenazas**, actualizaciones de **WildFire**, actualizaciones de archivos de datos de GlobalProtect y actualizaciones de bases de datos de **Filtrado de URL** de BrightCloud.

</td><td>

1. Seleccione **Panorama > Device Deployment (Implementación de dispositivos) > Actualizaciones dinámicas**.
2. Compruebe las actualizaciones más recientes. Haga clic en **Comprobar ahora** (ubicado en la esquina inferior izquierda de la ventana) para comprobar las actualizaciones más recientes. El enlace de la columna **Acción** indica si una actualización está disponible. Si hay una versión disponible, aparecerá en enlace **Descargar**; para la base de datos de Filtrado de URL de BrightCloud, el enlace aparecerá como **Actualizar**.

3. Haga clic en **Descargar** para descargar una versión seleccionada. Tras una descarga correcta, el enlace de la columna **Acción** cambia de **Descargar** a **Instalar**.
4. Haga clic en **Instalar** y seleccione los dispositivos en los que desee instalar la actualización. Cuando se complete la instalación, aparecerá una marca de verificación en la columna **Instalado actualmente**.

</td></tr>
<tr><td>

Implemente actualizaciones de software.

Para un recopilador gestionado, utilice la imagen que se corresponda con el nombre de plataforma **m**; para un dispositivo gestionado, busque la imagen que se corresponda con el modelo de hardware, por ejemplo, **5000**.

Este ejemplo le muestra cómo instalar una actualización de software PAN-OS. El cliente SSL VPN [**Panorama > Device Deployment (Implementación de dispositivos) > Cliente SSL VPN**] y el cliente de GlobalProtect [**Panorama > Device Deployment (Implementación de dispositivos) > Cliente de GlobalProtect**] utilizan el mismo mecanismo. Sin embargo, no *instala* el software en el cortafuegos; por el contrario, lo *activa* en el cortafuegos para que pueda descargarse en sistemas cliente.

</td><td>

1. Seleccione **Panorama > Device Deployment (Implementación de dispositivos) > Software**.
2. Compruebe las actualizaciones más recientes. Haga clic en **Comprobar ahora** (ubicado en la esquina inferior izquierda de la ventana) para comprobar las actualizaciones más recientes. El enlace de la columna **Acción** indica si una actualización está disponible.
3. Revise el **Nombre de archivo** y haga clic en **Descargar**. Verifique que las versiones de software que ha descargado coinciden con los modelos de cortafuegos implementados en su red. Tras una descarga correcta, el enlace de la columna **Acción** cambia de **Descargar** a **Instalar**.
4. Haga clic en **Instalar** y seleccione los dispositivos en los que desee instalar la versión de software. El resultado del intento de instalación se mostrará en pantalla.
Nota Puede descargar un máximo de cinco versiones de software por categoría en Panorama. Después de cinco versiones, cuando se inicia una nueva descarga, la imagen más antigua se elimina automáticamente.

</td></tr>
<tr><td>

Verifique la versión de actualización de contenido y de software que se ejecutan en cada dispositivo gestionado.

</td><td>

1. Seleccione **Panorama > Dispositivos gestionados**.
2. Ubique los dispositivos y revise el contenido y las versiones de contenido y de software en la tabla.

</td></tr>
</table>

Device Group	Device Name	Conn...	Status: Template	Software Version	Apps and Threat	Antivirus	URL Filtering	GlobalProtect Client	WildFire
Branch (1/1 Devices Connected)									
Branch	SupportFW-07	✓	In sync	5.0.0	347-1647	862-1186	4061	1.1.3	15901-23121

IMPLEMENTACIÓN DE SOFTWARE Y LICENCIAS EN DISPOSITIVOS GESTIONADOS MEDIANTE PANORAMA (CONTINUACIÓN)

Verifique la versión de actualización de contenido y de software que se ejecutan en cada recopilador gestionado.

1. Para verificar la versión de un recopilador gestionado, debe acceder a la CLI del recopilador gestionado. Consulte Inicio de sesión en la CLI.
2. Introduzca el comando **`show system info`**.

   Debe aparecer la siguiente información detallada:

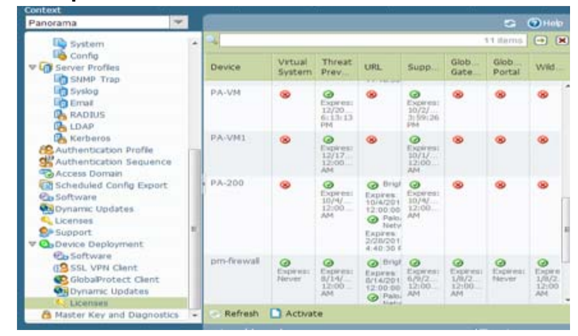
```
sw-version: 5.1.0-b10
app-version: 366-1738
app-release-date: 2013/03/29  15:46:03
av-version: 1168-1550
av-release-date: 2013/04/21  14:31:27
threat-version: 366-1738
threat-release-date: 2013/03/29  15:46:03
```

- Implemente las licencias.

  Cada entrada en la pestaña **Panorama > Device Deployment (Implementación de dispositivos) > Licencias** indica si la licencia está activa o inactiva; también muestra la fecha de vencimiento de las licencias activas.

Nota No puede utilizar Panorama para activar la licencia de asistencia técnica de los dispositivos gestionados.

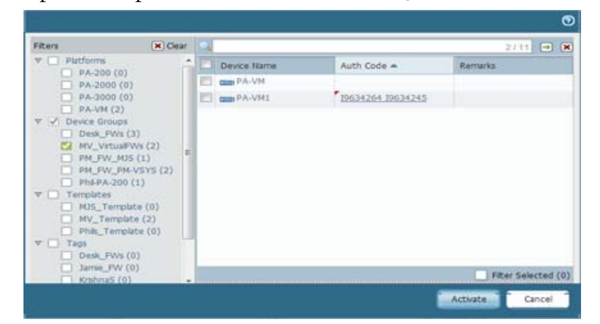
1. Seleccione **Panorama > Device Deployment (Implementación de dispositivos) > Licencias**.



2. Si ha activado anteriormente el código de autorización para la suscripción a la asistencia técnica directamente en el cortafuegos, haga clic en **Actualizar** y seleccione uno o más dispositivos de la lista. Panorama recupera las licencias, las implementa en los dispositivos gestionados y actualiza el estado de licencia en la interfaz web de Panorama.

Nota Esta capacidad de recuperar e implementar licencias mediante Panorama es de especial utilidad para las renovaciones de licencia de dispositivos que no tienen un acceso directo a Internet.

3. Para activar nuevas licencias:
   a. Haga clic en **Activar**. Esta opción le permite activar una suscripción recién adquirida, por ejemplo, una suscripción a amenaza.
   b. Busque o filtre los dispositivos gestionados e introduzca los códigos de autenticación que Palo Alto Networks proporcionó para el dispositivo en la columna **Código de autenticación**.

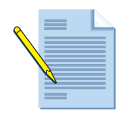


   c. Haga clic en **Activar**.

Sustitución de un dispositivo gestionado por un nuevo dispositivo

Para reducir al mínimo el esfuerzo necesario para restablecer la configuración de un dispositivo gestionado en una autorización de devolución de mercancía, puede sustituir el número de serie del dispositivo anterior por el del dispositivo nuevo/de sustitución en Panorama. Para a continuación restablecer la configuración en el dispositivo de sustitución, puede importar un estado de dispositivo que haya generado y exportado anteriormente del dispositivo o puede utilizar Panorama para generar un *estado de dispositivo* parcial para dispositivos gestionados que ejecuten PAN-OS v5.0 y versiones posteriores. El estado de dispositivo parcial que cree replica la configuración de los dispositivos gestionados con un par de excepciones para configuraciones de VPN a gran escala (LSVPN). Se crea combinando dos facetas de la configuración en un dispositivo gestionado:

- Configuración centralizada gestionada por Panorama: Panorama mantiene una instantánea de las políticas y plantillas compartidas introducidas desde Panorama.
- Configuración local del dispositivo: Cuando se compila un cambio de configuración, cada dispositivo envía una copia de su archivo de configuración local a Panorama. Este archivo se almacena en Panorama y se utiliza para compilar el lote del estado de dispositivo parcial.



En una configuración de LSVPN, el lote del estado de dispositivo parcial que genera en Panorama no es el mismo que la versión que puede exportar usando la operación **Exportar estado de dispositivo** desde la pestaña **Dispositivo > Configuración > Operaciones** en el cortafuegos. Si ha ejecutado manualmente la exportación de estado de dispositivo o ha programado un comando API XML para exportar el archivo a un servidor remoto, puede utilizar el estado de dispositivo exportado de su flujo de trabajo de sustitución de dispositivo a continuación.

Si no ha exportado el estado de dispositivo, el estado de dispositivo que genere en este flujo de trabajo no incluirá la información de configuración dinámica, como la información detallada de certificado y los dispositivos registrados, que es necesaria para restablecer la configuración completa de un dispositivo que funcione como portal de LSVPN. Consulte Antes de comenzar para obtener más información.

El estado de dispositivo no se almacena en Panorama; se genera tras su solicitud mediante los comandos de la CLI enumerados en Restablecimiento de la configuración en el nuevo dispositivo. Al sustituir el número de serie e importar el estado de dispositivo, puede volver a gestionar el dispositivo con Panorama.

Antes de comenzar

- El dispositivo gestionado (que se sustituyó) debe ejecutar PAN-OS v5.0.4 o una versión posterior. Panorama no puede generar el *estado de dispositivo* para dispositivos que ejecuten versiones anteriores de PAN-OS. Si necesita restablecer la configuración para un dispositivo que ejecute una versión de PAN-OS anterior a 5.0.4, consulte este artículo: Configuration Recovery with Panorama (Recuperación de configuración con Panorama).

- Anote la siguiente información detallada del dispositivo anterior:
  - **Número de serie**: Deberá introducir el número de serie en el portal de asistencia técnica para transferir las licencias del dispositivo anterior al dispositivo de sustitución. También deberá introducir esta información en Panorama para sustituir todas las referencias al número de serie anterior por el número de serie del dispositivo de sustitución.
  - (Recomendado) **Versión de PAN-OS y versión de la base de datos de contenido**: La instalación de las mismas versiones de software y base de datos de contenido, incluido el proveedor de base de datos de URL, le permite crear el mismo estado en el dispositivo de sustitución. Si decide instalar la versión más reciente de la base de datos de contenido, puede que observe diferencias debido a actualizaciones y adiciones a la base de datos. Para verificar las versiones instaladas en el dispositivo, acceda a los logs de sistema del dispositivo almacenados en Panorama.
- Prepare el dispositivo de sustitución para su implementación. Antes de importar el lote del estado de dispositivo y restablecer la configuración, debe hacer lo siguiente:
  - Verifique que el dispositivo de sustitución es del mismo modelo y está habilitado para una capacidad operativa similar. Considere las siguientes funciones operativas: ¿debe habilitarse para varios sistemas virtuales, admitir tramas gigantes o habilitarse para funcionar en modo CC o FIPS?
  - Configure el acceso de red, transfiera las licencias e instale la versión de PAN-OS y la versión de la base de datos de contenido adecuadas.
- Debe utilizar la CLI de Panorama para completar este proceso de sustitución de dispositivo. Este flujo de trabajo basado en la CLI está disponible para las funciones de usuario *Superusuario* y *Administrador de Panorama*.
- Si tiene una configuración de LSVPN y está sustituyendo un cortafuegos de Palo Alto Networks implementado como dispositivo satélite o portal de LSVPN, la información de configuración dinámica necesaria para restablecer la conectividad de LSVPN no estará disponible cuando restablezca el estado de dispositivo parcial generado en Panorama. Si ha seguido la recomendación de generar y exportar frecuentemente el estado de dispositivo de los dispositivos de una configuración de LSVPN, utilice el estado de dispositivo que había exportado anteriormente desde el propio dispositivo en lugar de generar uno en Panorama.

  Si no ha exportado manualmente el estado de dispositivo desde el dispositivo y necesita generar un estado de dispositivo parcial en Panorama, la configuración dinámica que falta afectará al proceso de sustitución del dispositivo del modo siguiente:
  - **Si el dispositivo que está sustituyendo es un dispositivo de portal** que está configurado explícitamente con el número de serie de los dispositivos satélite (**Red > GlobalProtect > Portales > Configuración Satélite**), al restablecer la configuración del dispositivo, aunque se haya perdido la configuración dinámica, el dispositivo de portal podrá autenticar los dispositivos satélite correctamente. La autenticación correcta añadirá la información de configuración dinámica y la conectividad de LSVPN volverá a establecerse.
  - **Si está sustituyendo un dispositivo satélite**, el dispositivo satélite no podrá conectarse ni realizar la autenticación en el portal. Este fallo de conexión se produce porque el número de serie no se configuró explícitamente en el dispositivo (**Red > GlobalProtect > Portales > Configuración Satélite**) o porque, aunque el número de serie se configuró explícitamente, el número de serie del dispositivo sustituido no coincide con el del dispositivo anterior. Para restablecer la conectividad, después de importar el lote del estado de dispositivo, el administrador del satélite debe iniciar sesión en el dispositivo e introducir las credenciales (nombre de usuario y contraseña) para realizar la autenticación en el portal. Cuando se produzca esta autenticación, la configuración dinámica necesaria para la conectividad de LSVPN se generará en el portal.

  Sin embargo, si el dispositivo tiene una configuración de alta disponibilidad, después de restablecer la configuración, el dispositivo sincronizará automáticamente la configuración que se está ejecutando con su peer y obtendrá la configuración dinámica más reciente necesaria para funcionar sin problemas.

Restablecimiento de la configuración en el nuevo dispositivo

Utilice el siguiente flujo de trabajo para restablecer la configuración del dispositivo.

RESTABLECIMIENTO DE LA CONFIGURACIÓN DEL DISPOSITIVO

▲ Tareas en el nuevo dispositivo
Utilice la CLI para lograr un flujo de trabajo más dinámico.

Paso 1.	Realice la configuración inicial y verifique la conectividad de red.	Utilice una conexión de puerto de serie o una conexión de SSH para añadir una dirección IP y una dirección IP de un servidor DNS y para verificar que el dispositivo puede acceder al servidor de actualizaciones de Palo Alto Networks. Para obtener instrucciones, consulte la *Palo Alto Networks Getting Started Guide (Guía de inicio de Palo Alto Networks)*.
Paso 2	(Opcional) Establezca el modo de operación que coincida con el del dispositivo anterior. Se requiere una conexión de puerto de serie para esta tarea.	1. Introduzca el siguiente comando de la CLI para acceder al modo de mantenimiento del dispositivo: **`debug system maintenance-mode`** 2. Para arrancar en la partición de mantenimiento, introduzca **`maint`** durante la secuencia de arranque. 3. Seleccione el modo operativo como **Establecer modo FIPS** o **Set CCEAL 4 Mode (Establecer modo CCEAL 4)** desde el menú principal.
Paso 3	Recupere las licencias.	Introduzca el siguiente comando para recuperar sus licencias: **`request license fetch`**
Paso 4	(Opcional) Haga coincidir el estado operativo del nuevo dispositivo con el del dispositivo anterior. Por ejemplo, habilite la capacidad de varios sistemas virtuales (VSYS múltiple) para un dispositivo que tuviera esta capacidad habilitada.	Introduzca los comandos relativos a sus ajustes de dispositivo: **`set system setting multi-vsys on`** **`set system setting jumbo-frame on`**
Paso 5	Actualice la versión de PAN-OS en el dispositivo. Debe actualizar a las mismas versiones del sistema operativo y la base de datos de contenido que las instaladas en el dispositivo anterior.	Introduzca los siguientes comandos: 1. Para actualizar la versión de la base de datos de contenido: **`request content upgrade download <xxx-xxxx>`** 2. Para instalar la versión de la base de datos de contenido que ha descargado: **`request content upgrade install version <xxx-xxxx>`** 3. Para actualizar la versión del software PAN-OS: **`request system software download version 5.x.x`** 4. Para instalar la versión de la base de datos de contenido que ha descargado: **`request system software install version 5.x.x`**

RESTABLECIMIENTO DE LA CONFIGURACIÓN DEL DISPOSITIVO (CONTINUACIÓN)

▲ Tareas en la CLI de Panorama

No puede realizar estas tareas en la interfaz web de Panorama.

Paso 6 Sustituya el número de serie del dispositivo anterior por el del nuevo dispositivo de sustitución en Panorama. Al sustituir el número de serie en Panorama permite que el nuevo dispositivo se conecte a Panorama después de restablecer la configuración en el dispositivo.	1. Introduzca el siguiente comando en el modo de operación: **replace device old *<n.° de serie anterior>* new *<n.° de serie nuevo>*** 2. Vaya al modo de configuración y compile sus cambios. **configure** **commit** 3. Salga del modo de configuración.
(Omita este paso si ha exportado manualmente el estado de dispositivo desde su cortafuegos y vaya al Paso 8 a continuación.) Paso 7 Exporte el lote del estado de dispositivo a un ordenador mediante SCP o TFTP. El comando de exportación genera el lote del estado de dispositivo como un archivo comprimido tar y lo exporta a la ubicación especificada. Este estado de dispositivo no incluirá la configuración dinámica de LSVPN (información de satélite e información detallada de certificado).	Introduzca uno de los siguientes comandos: **scp export device-state device <n.° de serie nuevo> to <inicio de sesión> @ <IP de servidor>: <ruta>** o **tftp device-state device <n.° de serie nuevo> to <inicio de sesión> @ <IP de servidor>: <ruta>**

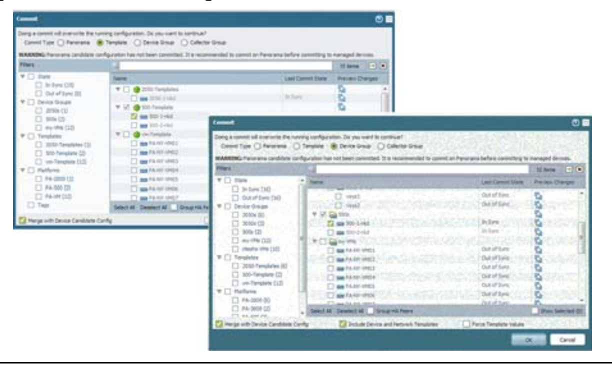
▲ Tareas en el nuevo dispositivo

Paso 8 Importe el estado de dispositivo y compile los cambios en el dispositivo.	1. Acceda a la interfaz web del dispositivo. 2. Seleccione **Dispositivo > Configuración > Operaciones** y haga clic en el enlace **Importar estado de dispositivo** en la sección Gestión de configuración. 3. Navegue para ubicar el archivo y haga clic en **ACEPTAR**. 4. Haga clic en **Compilar** para guardar los cambios en la configuración que se está ejecutando en el dispositivo. 5. Para confirmar que el estado de dispositivo restablecido incluye las referencias a las políticas y los objetos introducidos por Panorama, busque el icono pequeño de color verde . 

RESTABLECIMIENTO DE LA CONFIGURACIÓN DEL DISPOSITIVO (CONTINUACIÓN)

▲ Tareas en Panorama

Ahora puede utilizar la interfaz web de Panorama para acceder y gestionar el dispositivo sustituido.

Paso 9 Verifique que la configuración del dispositivo se haya restablecido correctamente.	1. Acceda a la interfaz web de Panorama. 2. Verifique que el nuevo dispositivo está conectado a Panorama.  3. Realice una compilación de plantillas y grupos de dispositivos para mantener el dispositivo sincronizado con Panorama. 



Después de sustituir el dispositivo, si necesita generar informes para un periodo que abarque el tiempo durante el cual el dispositivo anterior era funcional y después de haber instalado el dispositivo de sustitución, debe generar una consulta separada para cada número de serie de dispositivo, ya que sustituir el número de serie en Panorama no sobrescribe la información en los logs.

Transición de un dispositivo a una gestión central

Si ya ha implementado cortafuegos de Palo Alto Networks y los ha configurado localmente pero ahora desea empezar a utilizar Panorama para gestionarlos centralmente, cuenta con tareas de planificación anterior a la migración, implementación y verificación posterior a la migración. Esta descripción general de alto nivel no trata todas las tareas críticas necesarias para planificar, implementar y validar la transición a una administración centralizada. Estas son las actividades de planificación y configuración de alto nivel:

- En Panorama, añada los dispositivos y cree grupos de dispositivos para reunir lógicamente cortafuegos o sistemas virtuales que realicen una función parecida o que tengan características similares.
- Cree zonas comunes para cada grupo de dispositivos. Decida la estrategia de denominación de zonas comunes para todos los dispositivos y sistemas virtuales de un grupo de dispositivos. Por ejemplo, si tiene dos zonas denominadas LAN y WAN de sucursal, Panorama puede introducir centralmente políticas que hagan referencia a esas zonas sin tener en cuenta las variaciones en el tipo de puerto/medio, la plataforma o el esquema de dirección lógica. Debe crear las zonas en cada dispositivo gestionado antes de poder compilar los cambios en el grupo de dispositivos o plantilla. Panorama no puede sondear los dispositivos para conocer el nombre de zona o la configuración.
- Configure cada dispositivo para comunicarse con Panorama. Debe definir las direcciones IP de Panorama (principal y secundaria de Panorama) en cada dispositivo.
- Utilice grupos de dispositivos para crear políticas comunes para dispositivos con funciones parecidas y utilice plantillas para definir una configuración básica común para el dispositivo gestionado.
- Determine cómo gestionará reglas locales y excepciones específicas de dispositivo en ajustes de configuración y políticas comunes. Si tiene la intención de utilizar reglas configuradas localmente en los dispositivos, asegúrese de que los nombres de las reglas son exclusivos. Una buena forma de garantizarlo sería añadir un sufijo o prefijo a todas las reglas existentes.
- Considere eliminar todas las "reglas de denegación" en la política de seguridad local y utilice reglas posteriores de Panorama. Este enfoque le permite deshabilitar temporalmente reglas locales y comprobar las reglas posteriores compartidas introducidas desde Panorama. A continuación, puede probar las reglas posteriores, realizar los ajustes necesarios y eliminar la administración local en el dispositivo.
- Valide que los cortafuegos funcionan de manera eficaz con una configuración introducida por Panorama igual que hacían con una configuración local.

Para obtener información detallada sobre cómo utilizar la API REST basada en XML para completar la transición, consulte el siguiente documento: Panorama Device Migration (Migración de dispositivos de Panorama). Because Palo Alto Networks Technical Support does not help troubleshoot issues when using the XML API, if you do not have experience with scripting/using the XML API, contact Palo Alto Networks Professional Services to learn about the device migration process.

4 Supervisión de la actividad de red

Panorama ofrece una visión gráfica global del tráfico de red. Utilizando las herramientas de visibilidad en Panorama [el Centro de comando de aplicación (ACC), logs y las funciones de generación de informes] puede analizar, investigar y elaborar informes de manera central sobre toda la actividad de red, identificar áreas con un posible impacto en la seguridad y traducirlas a políticas de activación de aplicaciones seguras.

Esta sección cubre los siguientes temas:

- Uso de Panorama para lograr visibilidad
- Caso de uso: supervisión de aplicaciones mediante Panorama
- Caso de uso: uso de Panorama para responder a un incidente

Uso de Panorama para lograr visibilidad

Además de sus funciones de implementación central y configuración de dispositivos, Panorama también le permite supervisar y elaborar informes sobre todo el tráfico que atraviesa su red. Aunque las funciones de elaboración de informes de Panorama y el cortafuegos son muy parecidas, la ventaja de Panorama es que es una única vista de panel de información agregada de todos sus cortafuegos gestionados. Esta vista agregada ofrece información útil sobre tendencias en la actividad del usuario, patrones de tráfico y amenazas potenciales en toda su red.

Mediante el Centro de comando de aplicación (ACC), Appscope, el visor de logs y las opciones de elaboración de informes estándar y personalizables de Panorama, puede obtener más información rápidamente sobre el tráfico que atraviesa la red. La capacidad de ver esta información le permite evaluar en qué lugares sus políticas actuales son adecuadas y dónde son insuficientes. Luego podrá utilizar estos datos para aumentar su estrategia de seguridad de red. Por ejemplo, puede mejorar las reglas de seguridad para incrementar el cumplimiento y la responsabilidad de todos los usuarios a través de la red, o bien gestionar la capacidad de la red y reducir al mínimo los riesgos de los activos a la vez que cubre las numerosas necesidades de aplicaciones de los usuarios de su red.

Esta sección ofrece una visión de alto nivel de las capacidades de elaboración de informes en Panorama, incluido un par de casos de uso para mostrarle cómo puede utilizar estas capacidades en su propia infraestructura de red. Para obtener una lista completa de los informes y gráficos disponibles y la descripción de cada uno de ellos, consulte la ayuda en línea.

- ▲ Supervisión de la red con el ACC y Appscope
- ▲ Análisis de datos de log
- ▲ Generación de informes

Supervisión de la red con el ACC y Appscope

Tanto el ACC como Appscope le permiten supervisar y elaborar informes sobre los datos registrados del tráfico que atraviesa su red.

El ACC de Panorama muestra un resumen del tráfico de red. Panorama puede consultar datos dinámicamente desde todos los dispositivos gestionados en la red y mostrarlos en el ACC. Esta visualización le permite supervisar el tráfico por aplicaciones, usuarios y actividad de contenido (categorías de URL, amenazas, filtrado de datos, bloqueo de archivos, coincidencias HIP para GlobalProtect) a través de toda la red de cortafuegos de próxima generación de Palo Alto Networks.

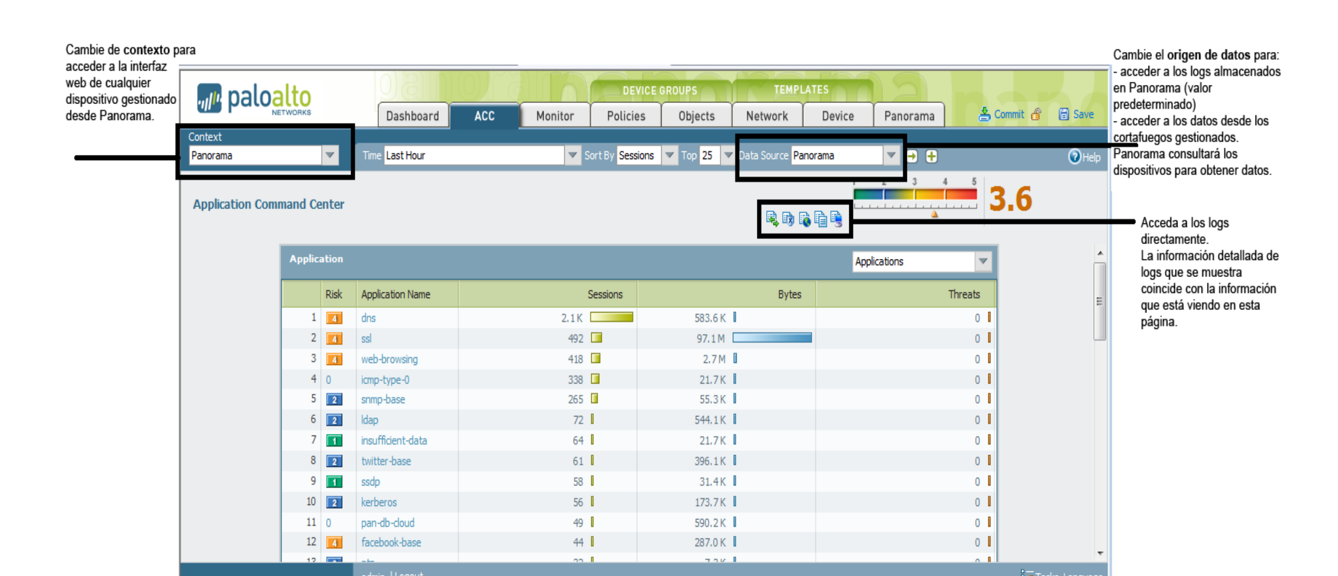
Appscope ayuda a identificar un comportamiento inesperado o inusual en la red de un vistazo. Incluye un conjunto de gráficos e informes (informe de resumen, supervisor de cambios, supervisor de amenazas, mapa de amenazas, supervisor de red, mapa de tráfico) que le permiten analizar flujos de tráfico por amenaza o aplicación, o bien por la fuente o el destino de los flujos. También puede ordenar por sesión o por recuento de bytes.

Utilice el ACC y Appscope para responder a preguntas como las siguientes:

ACC	**Supervisar > AppScope (Appscope)**
• ¿Cuáles son las principales aplicaciones utilizadas en la red y cuántas son aplicaciones de alto riesgo? ¿Quiénes son los principales usuarios de las aplicaciones de alto riesgo en la red? • ¿Cuáles son las principales categorías de URL que se visualizaron durante la última hora?	• ¿Cuáles son las tendencias de uso de aplicaciones? ¿Cuáles son las cinco principales aplicaciones que han aumentado su uso y las cinco principales que han disminuido su uso? • ¿Cómo ha cambiado la actividad de los usuarios a lo largo de la semana actual en comparación con la semana pasada o el mes pasado?
• ¿Cuáles son las principales aplicaciones que utilizan ancho de banda? ¿Cuáles son los usuarios/hosts que consumen el mayor ancho de banda? • ¿Qué contenido o archivos se están bloqueando? ¿Hay usuarios específicos que activan esta política de filtrado de datos/bloqueo de archivos? • ¿Cuál es la cantidad de tráfico intercambiado entre dos direcciones IP específicas o generado por un usuario específico? ¿Cuál es la ubicación geográfica del servidor o cliente de destino?	• ¿Qué usuarios y aplicaciones absorben la mayor parte del ancho de banda de la red? ¿Cómo ha cambiado este consumo durante los últimos 30 días?  • ¿Cuáles son las amenazas en la red y cómo se distribuyen geográficamente estas amenazas de tráfico de entrada y salida?

A continuación, podrá utilizar la información para mantener o aplicar cambios en los patrones de tráfico de su red. Consulte Caso de uso: supervisión de aplicaciones mediante Panorama para conocer brevemente cómo pueden influir las herramientas de visibilidad de Panorama en el modo en que moldea las políticas de uso aceptable para su red.

Aquí tiene algunos consejos que le ayudarán a navegar por el ACC:



- Cambio de una vista de Panorama a una vista de dispositivo: Panorama permite acceder a la interfaz web de cualquier dispositivo gestionado utilizando el menú **Contexto**. El cambio de contexto ofrece un acceso directo al cortafuegos; permite gestionar ajustes específicos del dispositivo, como una política específica del dispositivo, y/o cancelar la configuración de red implementada desde una plantilla de un dispositivo específico.

- **Cambio de origen de datos**: El origen predeterminado utilizado para visualizar las estadísticas de los gráficos del ACC son los datos locales de Panorama. A excepción de los datos mostrados en el gráfico **Aplicación**, el resto de gráficos requiere que habilite el reenvío de logs a Panorama.

  El uso de datos locales en Panorama permite cargar rápidamente los gráficos. No obstante, puede cambiar el origen de datos a **Remote Device Data (Datos de dispositivo remoto)**. Cuando se configura para utilizar datos de un dispositivo remoto en lugar de utilizar los datos locales de Panorama, Panorama sondeará todos los dispositivos gestionados y presentará una vista agregada de los datos. La visualización en pantalla muestra el número total de dispositivos que se están sondeando y el número de dispositivos que han respondido a la consulta de información.

- **Selección de los gráficos que se visualizarán**: El ACC incluye un conjunto de gráficos en las áreas de aplicaciones, filtrado de URL, prevención de amenazas, filtrado de datos y coincidencias HIP. A excepción de los gráficos de aplicaciones y las coincidencias HIP, el resto de gráficos solamente aparecen si la función correspondiente tiene licencia en el dispositivo y el usuario ha habilitado el registro.

- **Ajuste del período de tiempo y ordenación de datos**: El período de tiempo de elaboración de informes en el ACC va desde los últimos 15 minutos hasta la última hora, día, semana, mes o cualquier período de tiempo personalizado. Puede ordenar los datos por sesiones, bytes o amenazas y filtrarlos para ver de 5 a 500 elementos.

Análisis de datos de log

La pestaña **Supervisar** de Panorama permite acceder a datos de logs; estos logs son una lista archivada de sesiones que han sido procesadas por los cortafuegos gestionados y reenviadas a Panorama.

Los datos de logs pueden agruparse ampliamente en dos tipos: los que dan información detallada sobre los flujos de tráfico en su red como aplicaciones, amenazas, perfiles de información de host, categorías de URL, tipos de contenido/archivo y los que registran eventos del sistema, cambios de configuración y alarmas.

Basándose en la configuración de reenvío de logs de los dispositivos gestionados, la pestaña **Supervisar > Logs** puede incluir logs de flujos de tráfico, amenazas, filtrado de URL, filtrado de datos, coincidencias HIP (perfil de información de host) y presentaciones de WildFire. Puede revisar los logs para verificar una gran cantidad de información sobre una sesión o transacción específica, como los puertos, zonas y direcciones de origen y destino, el usuario que inició la sesión y la acción (permitir, negar) realizada por el cortafuegos en esa sesión; los logs de configuración y sistema pueden informarle de un cambio de configuración o una alarma activada cuando se superó un umbral configurado.

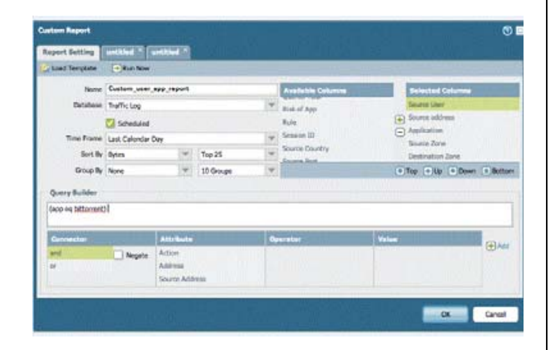
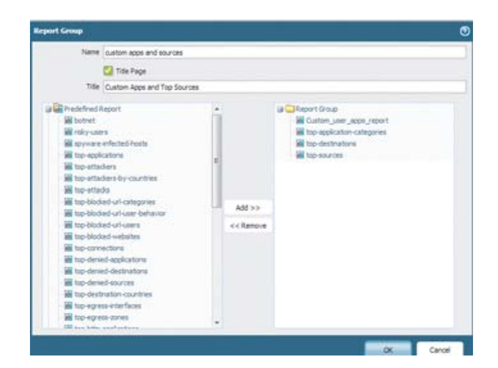
Generación de informes

Panorama le permite generar informes manualmente según sea necesario o programar que se ejecuten informes a intervalos específicos. Puede guardar y exportar informes o puede configurar Panorama para que envíe informes por correo electrónico a destinatarios específicos. La capacidad de compartir informes mediante el correo electrónico es de especial utilidad si desea compartir información de informes con administradores que no tengan acceso a Panorama.

Puede crear los siguientes tipos de informes:

- **Informes predefinidos**: Hay disponible un conjunto de informes predefinidos en cuatro categorías: Applications (Aplicaciones), Threats (Amenazas), Filtrado de URL y Traffic (Tráfico), en la pestaña **Supervisar > Reports (Informes)**.
- **Informes de actividad del usuario**: El informe de actividad del usuario es un informe predefinido que se utiliza para crear un informe a petición para documentar el uso de aplicaciones y la actividad de URL desglosada por categoría de URL para un usuario específico con cálculos de tiempo de exploración estimados. Este informe está disponible en la pestaña **Supervisar > Informes en PDF > User Activity Reports (Informes de actividad del usuario)**.
- **Informes personalizados**: Cree y programe informes personalizados que muestren exactamente la información que desee ver, filtrando según las condiciones y las columnas que deben incluirse. Puede generar informes para consultar datos de una base de datos de resumen de Panorama o de los dispositivos remotos (es decir, los cortafuegos gestionados) o utilizar los informes detallados de Panorama o de los dispositivos remotos. Para ver las bases de datos disponibles para generar estos informes, consulte la pestaña **Supervisar > Gestionar informes personalizados**. También puede crear grupos de informes (pestaña **Supervisar >Informes en PDF > Grupos de informes**) para compilar informes predefinidos e informes personalizados como un único PDF.
- **Informes de resumen en PDF**: Agregue hasta 18 informes predefinidos, gráficos e informes personalizados a un documento PDF.

La siguiente tabla ofrece instrucciones paso a paso para crear y programar informes:

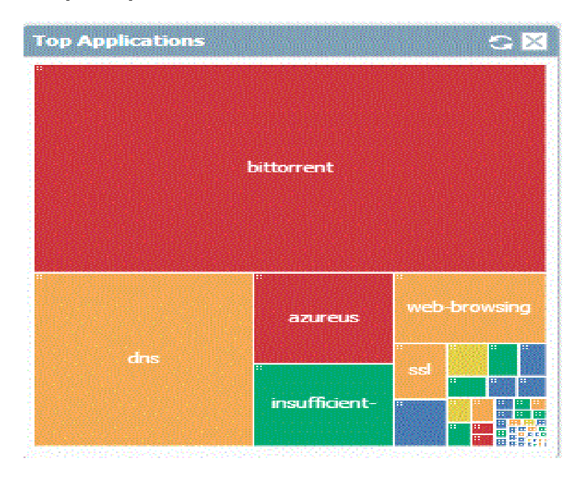
GENERACIÓN, PROGRAMACIÓN Y ENVÍO POR CORREO ELECTRÓNICO DE INFORMES	
Paso 1. Genere informes. **Nota** Debe configurar un **Grupo de informes** para enviar informes por correo electrónico.  	• Cree un informe personalizado. a. Seleccione **Supervisar > Gestionar informes personalizados**. b. Haga clic en **Añadir** y, a continuación, introduzca un **Nombre** para el informe. c. Seleccione la base de datos, **Panorama** o **Remote Device Data (Datos de dispositivo remoto)** que desee utilizar para el informe. Puede utilizar la base de datos de resumen o los logs detallados de Panorama o de los dispositivos gestionados. d. Seleccione la casilla de verificación **Programado**. e. Defina sus criterios de filtrado. Seleccione el **Período de tiempo**, el orden **Ordenar por** y la preferencia **Agrupar por** y seleccione las columnas que deben mostrarse en el informe. f. (Opcional) Seleccione los atributos **Generador de consultas** si desea ajustar aun más los criterios de selección. g. Para comprobar los ajustes de informes, seleccione **Ejecutar ahora**. Modifique los ajustes según sea necesario para cambiar la información que se muestra en el informe. h. Haga clic en **ACEPTAR** para guardar el informe personalizado. • Ejecute un **Informe de resumen en PDF**. a. Seleccione **Supervisar > Informes en PDF > Gestionar resumen de PDF**. b. Haga clic en **Añadir** y, a continuación, introduzca un **Nombre** para el informe. c. Utilice la lista desplegable para cada grupo de informes y seleccione uno o más de los elementos para diseñar el informe de resumen en PDF. Puede incluir un máximo de 18 elementos de informe. d. Haga clic en **ACEPTAR** para guardar los ajustes. • Defina el **Grupo de informes**. Puede incluir informes predefinidos, informes de resumen en PDF e informes personalizados. Panorama compila todos los informes incluidos en un único PDF. a. Seleccione **Supervisar > Grupo de informes**. b. Haga clic en **Añadir** y, a continuación, introduzca un **Nombre** para el grupo de informes. c. (Opcional) Seleccione **Página de título** y añada un **Título** para el PDF creado. d. Seleccione informes en las listas Informe predefinido, Informe de resumen en PDF e Informe personalizado; haga clic en **Añadir** para incluir los informes seleccionados en el grupo de informes. e. Haga clic en **ACEPTAR** para guardar la configuración.

GENERACIÓN, PROGRAMACIÓN Y ENVÍO POR CORREO ELECTRÓNICO DE INFORMES (CONTINUACIÓN)		
Paso 2	Configure Panorama para enviar informes por correo electrónico.	1. Seleccione **Panorama > Perfiles de servidor > Correo electrónico**. 2. Haga clic en **Añadir** y, a continuación, introduzca un **Nombre** para el perfil. 3. Haga clic en **Añadir** para añadir una nueva entrada de servidor de correo electrónico e introduzca la información necesaria para conectar con el servidor SMTP y enviar mensajes de correo electrónico (puede añadir hasta cuatro servidores de correo electrónico al perfil): • **Servidor**: Nombre para identificar el servidor de correo electrónico (1-31 caracteres). Este campo es solamente una etiqueta y no tiene que ser el nombre de host de un servidor SMTP existente. • **Email Display Name (Nombre de visualización de correo electrónico)**: El nombre que aparecerá en el campo De del correo electrónico. • **De**: La dirección de correo electrónico desde la que se enviarán las notificaciones de correo electrónico. • **Para**: La dirección de correo electrónico a la que se enviarán las notificaciones de correo electrónico. • **Additional Recipient (Destinatario adicional)**: Si desea que las notificaciones se envíen a una segunda cuenta, introduzca la dirección adicional aquí. • **Email Gateway (Puerta de enlace de correo electrónico)**: La dirección IP o el nombre de host de la puerta de enlace SMTP que se usará para enviar los mensajes de correo electrónico. 4. Haga clic en **Aceptar** para guardar el perfil de servidor. 5. Haga clic en **Compilar** y seleccione **Panorama** en **Compilar tipo** para guardar los cambios en la configuración que se está ejecutando.
Paso 3	Programe la entrega del informe por correo electrónico.  	1. Seleccione **Supervisar > Informes en PDF > Programador de correo electrónico**. 2. Haga clic en **Añadir** y, a continuación, introduzca un **Nombre** para el perfil del programador de correo electrónico. 3. Seleccione el **Grupo de informes**, el **Perfil de correo electrónico** y la **Periodicidad** del informe. 4. Para verificar que los ajustes de correo electrónico son precisos, seleccione **Enviar correo electrónico de prueba**. 5. Haga clic en **Aceptar** para guardar la configuración.
Paso 4	Guarde los cambios de configuración.	Haga clic en **Compilar** y seleccione **Panorama** en **Compilar tipo** para guardar los cambios en la configuración que se esté ejecutando.

Caso de uso: supervisión de aplicaciones mediante Panorama

Este ejemplo le muestra todo el proceso de evaluación de la eficacia de sus políticas actuales y de determinación de los puntos donde necesita ajustarlas para fortalecer las políticas de uso aceptable para su red.

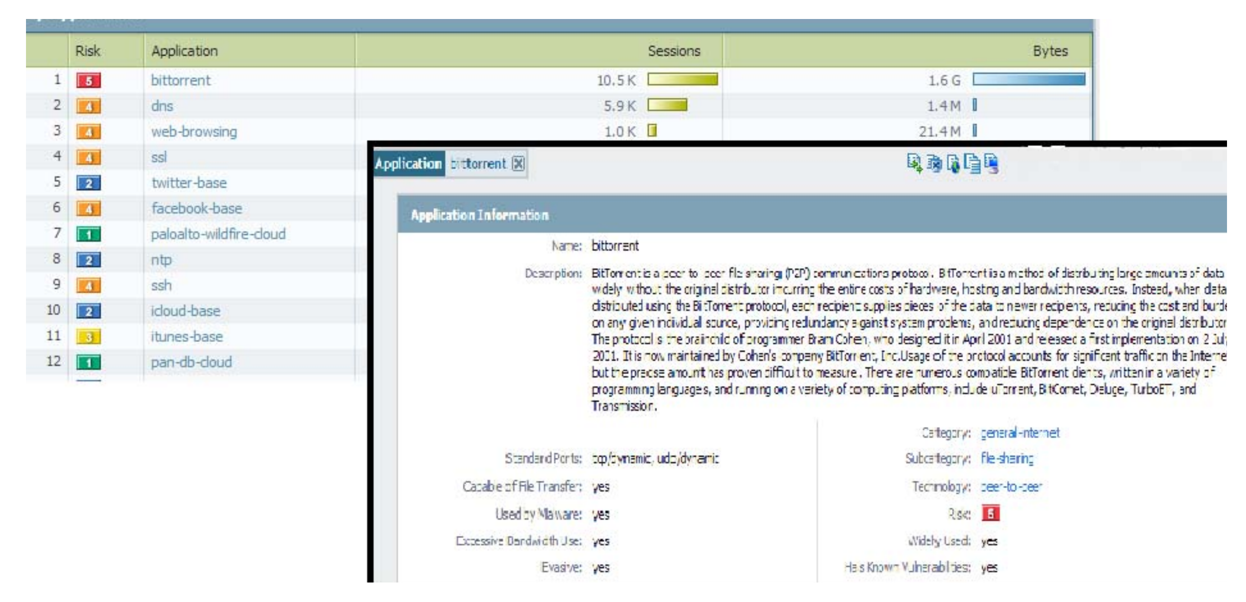
Cuando se registra en Panorama, el widget **Aplicaciones principales** del **Panel** ofrece una vista previa de las aplicaciones más utilizadas durante la última hora. Puede echar un vistazo a la lista de aplicaciones principales y pasar el ratón por encima de cada bloque de aplicación del que quiera obtener información detallada, o bien puede navegar hasta la pestaña **ACC** para ver la misma información en una lista ordenada. La siguiente imagen es una vista del widget **Aplicaciones principales** del **Panel**.



El origen de datos de esta visualización es la base de datos de estadísticas de aplicación; no utiliza los logs de tráfico y se genera haya o no habilitado los logs para reglas de seguridad. Esta visualización del tráfico de su red muestra todo lo que está permitido en su red y fluye sin bloqueos por parte de las reglas de políticas que haya definido.

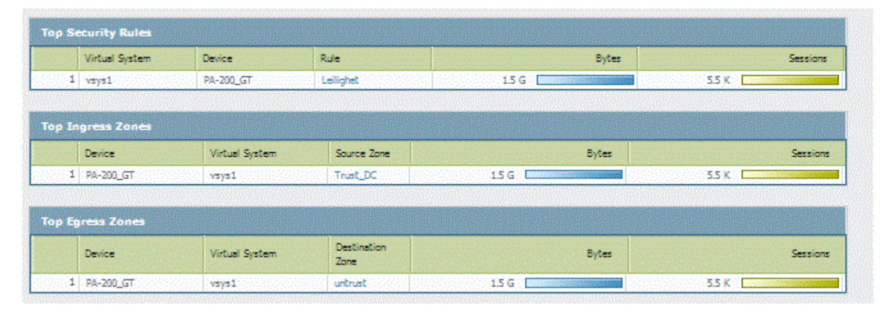
Puede seleccionar y cambiar **Data Source (Origen de datos)** para que sea local en Panorama o puede consultar los cortafuegos gestionados [**Remote Device Data (Datos de dispositivo remoto)**] para los datos; Panorama automáticamente agrega y muestra la información. Para lograr un flujo más veloz, considere utilizar Panorama como el origen de datos (con el reenvío de logs a Panorama habilitado), ya que el tiempo necesario para cargar datos desde los dispositivos remotos varía según el período de tiempo que seleccione para visualizar datos y el volumen de tráfico generado en su red.

Volviendo a la lista de aplicaciones principales, podemos observar que bittorrent es muy popular. Si ahora hace clic en el enlace de la aplicación bittorrent, la vista **ACC** filtrará la visualización para mostrar información sobre la aplicación, su comportamiento, su nivel de riesgo y los detalles de categorización de URL asociados.

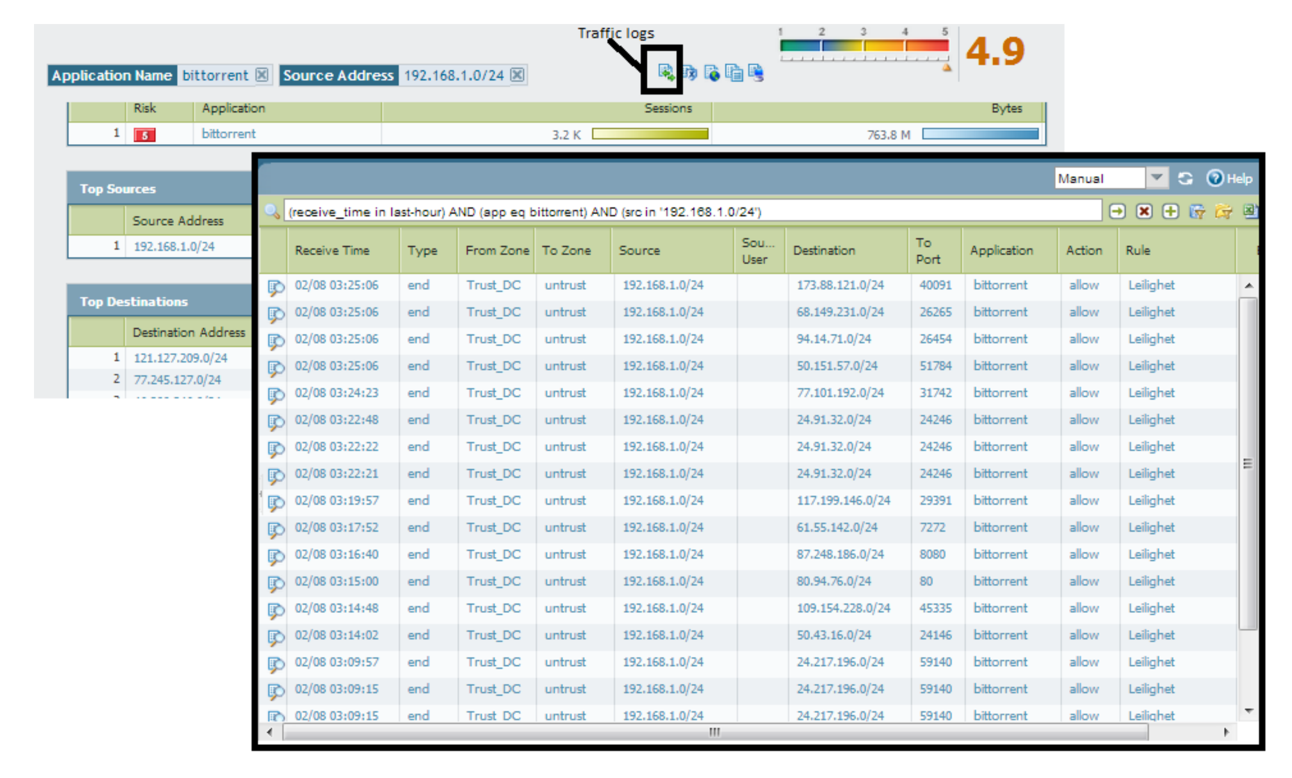


En la tabla **Orígenes principales**, también puede ver cuántos usuarios están utilizando bittorrent y el volumen de tráfico que se está generando. Si ha habilitado el ID de usuarios, podrá ver los nombres de los usuarios que están generando este tráfico. Ahora puede hacer clic en un usuario de origen y desglosarlo para revisar toda la actividad de ese usuario.

Mediante la vista **ACC** para filtrar el tráfico de bittorrent generado por el usuario o la dirección de origen específicos nos permite verificar el país de origen y destino de este tráfico, el dispositivo que está procesando este tráfico, las zonas de entrada y salida y la regla de seguridad que está permitiendo esta conexión.



Para obtener información más detallada, desglose los logs de tráfico para obtener una vista filtrada y revise cada entrada de log para conocer los puertos utilizados, los paquetes enviados y los bytes enviados y recibidos. Ajuste las columnas para ver más o menos información basándose en sus necesidades.



La pestaña **Supervisar > Appscope > Mapa de tráfico** muestra un mapa geográfico del flujo de tráfico y proporciona una vista del tráfico entrante frente al tráfico saliente. También puede utilizar la pestaña **Supervisar > Appscope > Supervisor de cambios** para ver los cambios en los patrones de tráfico. Por ejemplo, compare las aplicaciones principales utilizadas durante esta hora en comparación con la semana pasada o el mes pasado para determinar si hay un patrón o tendencia.

Con toda la información que ha descubierto, ahora puede evaluar qué cambios hacer en las configuraciones de sus políticas. Aquí tiene algunas sugerencias que considerar:

- Sea restrictivo y decida crear una *regla previa* en Panorama para bloquear todo el tráfico de bittorrent. A continuación, utilice grupos de dispositivos de Panorama para crear e introducir esta regla de política en uno o más dispositivos.

- Aplique límites de uso de ancho de banda y cree una *política y perfil de calidad de servicio (QoS)* que retire la prioridad del tráfico no comercial. A continuación, utilice plantillas de Panorama para introducir esta política en uno o más dispositivos. Consulte el artículo Panorama Templates (Plantillas de Panorama) para definir una política de calidad de servicio (QoS) mediante plantillas.

- Reduzca el riesgo en sus activos de red y cree un *filtro de aplicación* que bloquee todas las aplicaciones que compartan archivos que tengan una tecnología punto a punto con un factor de riesgo de 4 o 5. Asegúrese de verificar que la aplicación bittorrent está incluida en ese filtro de aplicación y que, por lo tanto, estará bloqueada.

- Programe un grupo de informes personalizados que recopile la actividad del usuario específico y de las aplicaciones principales utilizadas en su red para observar ese patrón durante una o dos semanas más antes de realizar una acción.

Además de comprobar una aplicación específica, también puede comprobar cualquier *aplicación desconocida* de la lista de aplicaciones principales. Son aplicaciones que no coinciden con una firma de ID de aplicaciones definida y aparecen como *UDP desconocido* y *TCP desconocido*. Para ahondar en estas aplicaciones desconocidas, haga clic en el nombre para desglosar los detalles del tráfico sin clasificar.

Utilice el mismo proceso para investigar las direcciones IP de origen principales de los hosts que iniciaron el tráfico *desconocido* junto con la dirección IP del host de destino para el que se estableció la sesión. Para el tráfico desconocido, los logs de tráfico, de manera predeterminada, realizan una captura de paquetes (PCAP) cuando se detecta una aplicación desconocida. La flecha verde de la columna de la izquierda representa el fragmento de código de captura de paquetes de los datos de la aplicación. Si hace clic en la flecha verde, mostrará la captura de paquetes (PCAP) en el explorador.

Ahora, con la combinación de las direcciones IP de los servidores (IP de destino en los logs), el puerto de destino y las capturas de paquetes, estará en una posición más privilegiada para identificar la aplicación y tomar una decisión sobre qué acción desea realizar en su red. Por ejemplo, puede crear una aplicación personalizada que identifique este tráfico en lugar de etiquetarlo como tráfico de TCP o UDP desconocido. Consulte el artículo Aplicaciones desconocidas para obtener más información sobre cómo identificar aplicaciones desconocidas y Custom Application Signature (Firma de aplicación personalizada) para obtener información sobre cómo desarrollar firmas personalizadas para distinguir la aplicación.

Caso de uso: uso de Panorama para responder a un incidente

Las amenazas de red pueden originarse desde diferentes vectores, incluidas infecciones de software malintencionado y spyware debidas a descargas ocultas, ataques de phishing, servidores sin la suficiente protección y sin parches y ataques de denegación de servicio (DoS) aleatorios o con destino específico, por nombrar unos cuantos métodos de ataque. La capacidad de reaccionar ante una infección o un ataque a la red requiere procesos y sistemas que avisen al administrador del ataque y proporcionen las pruebas expertas necesarias para realizar un seguimiento del origen y los métodos utilizados para lanzar el ataque.

La ventaja de Panorama es una vista centralizada y consolidada de los patrones y logs recopilados desde los cortafuegos gestionados de su red. Utilizada sola o en conjunto con los informes y logs generados desde un gestor de eventos, información y seguridad (SIEM), la información de ataque correlacionada puede utilizarse para investigar cómo se ha activado un ataque y cómo prevenir ataques futuros y pérdidas o daños en su red.

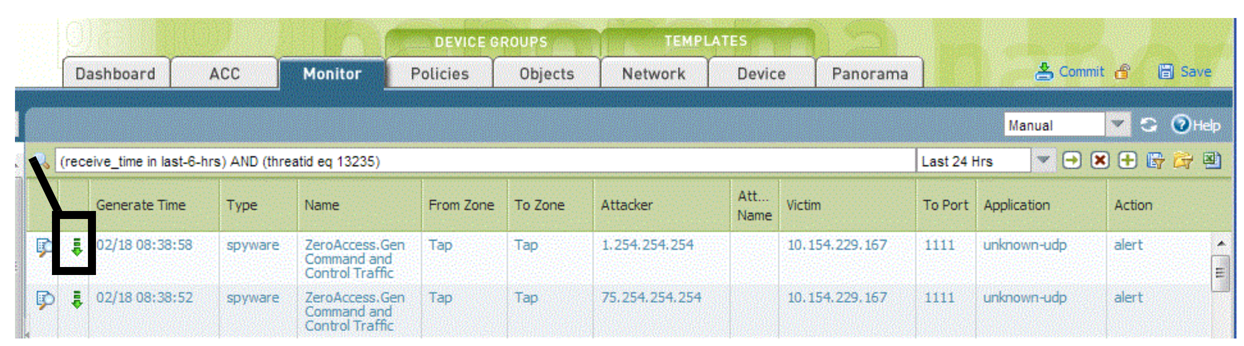
Las preguntas que exploraremos en esta sección son:

- ¿Cómo se le notifica un incidente?
- ¿Cómo corrobora que el incidente no es un falso positivo?
- ¿Cuál es su plan de acción inmediato?
- ¿Cómo utiliza la información disponible para reconstruir la secuencia de eventos que precedió o siguió al evento desencadenante?
- ¿Qué cambios debe considerar para proteger su red?

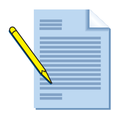
En este caso de uso, haremos un seguimiento a un incidente específico y le mostraremos de qué modo las herramientas de visibilidad de Panorama pueden ayudarle a responder al informe.

Se le puede avisar de varias formas de un incidente dependiendo de cómo haya configurado los dispositivos de Palo Alto Networks y de qué herramientas externas estén disponibles para un análisis posterior. Puede recibir una notificación por correo electrónico activada por una entrada de log registrada en Panorama o en su servidor Syslog, se le puede informar a través de un informe especializado generado en su solución SIEM, o bien una agencia o un servicio pagado externo puede notificarle. En este ejemplo, vamos a suponer que ha recibido una notificación de Panorama por correo electrónico. El mensaje de correo electrónico le informa de un evento activado por una alerta para **Zero Access gent.Gen Command And Control Traffic (Comando gent.Gen de acceso cero y tráfico de control)** que coincide con una firma de spyware. En el mensaje de correo electrónico también se indica la dirección IP del origen y el destino de la sesión, un ID de amenaza y la marca de tiempo de cuándo se registró el evento.

Para empezar a investigar la alerta, utilice el ID de amenaza para buscar los logs de amenaza en Panorama (**Supervisar > Logs > Amenaza**). Desde los logs de amenaza, puede buscar la dirección IP de la víctima, exportar la captura de paquetes (PCAP, con un icono de flecha verde en la entrada de log) y utilizar una herramienta de análisis de red como WireShark para revisar la información detallada del paquete. En el caso de HTTP, busque un SITIO DE REFERENCIA HTTP falso o con formato incorrecto en el protocolo, un host sospechoso, cadenas de URL, el agente del usuario, la dirección IP y el puerto para validar el incidente. Los datos de estas capturas de paquetes también son útiles para buscar patrones de datos similares y crear firmas personalizadas o modificar políticas de seguridad para enfrentarse mejor a la amenaza en el futuro.



Como resultado de esta revisión manual, si confía en la firma, considere trasladar la firma de una acción de alerta a una acción de bloqueo para un enfoque más agresivo. En algunos casos, puede decidir añadir el IP del atacante a una lista de bloqueo de IP para evitar que el tráfico de esa dirección IP vuelva a llegar a la red interna.



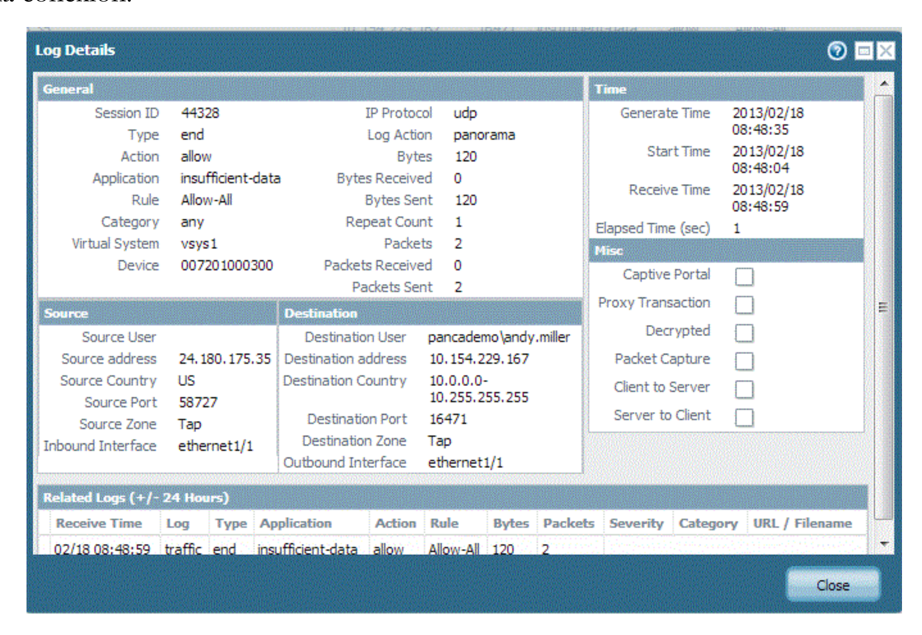
Si observa una firma de spyware basada en DNS, la dirección IP de su servidor DNS local podría aparecer como la dirección IP de la **Víctima**. A menudo esto se debe a que el cortafuegos se encuentra al norte del servidor DNS local, por lo que todas las consultas DNS muestran el servidor DNS local como la IP de origen, en lugar de mostrar la dirección IP del cliente que originó la solicitud. Si observa este problema, consulte los logs de DNS local para buscar el cliente desde el que se originó la consulta.

En el futuro, considere enrutar las solicitudes DNS de cliente directamente al cortafuegos para que este pueda registrar la dirección IP de la víctima con precisión.

Para continuar con la investigación del incidente, utilice la información del atacante y la dirección IP de la víctima para obtener información adicional, como la siguiente:

- ¿Cuál es la ubicación geográfica del atacante? ¿La dirección IP es una dirección IP individual o una dirección IP con NAT?
- ¿El evento fue provocado al engañar a un usuario para que entrara en un sitio web o realizara una descarga, o bien se envió a través de un archivo adjunto por correo electrónico?
- ¿Se está propagando el software malintencionado? ¿Hay otros hosts/extremos en peligro en la red?
- ¿Es una vulnerabilidad de día cero?

La información detallada de log de cada entrada de log muestra los **Registros relacionados** para el evento. Esta información le dirige a los logs de tráfico, amenaza, filtrado de URL u otros logs que puede revisar para correlacionar los eventos que dieron lugar al incidente. Por ejemplo, filtre el log de tráfico (**Supervisar > Logs > Traffic (Tráfico)**) usando la dirección IP como IP tanto de origen como de destino para obtener una imagen completa de todos los hosts/clientes externos e internos con los que esta dirección IP de la víctima haya establecido una conexión.



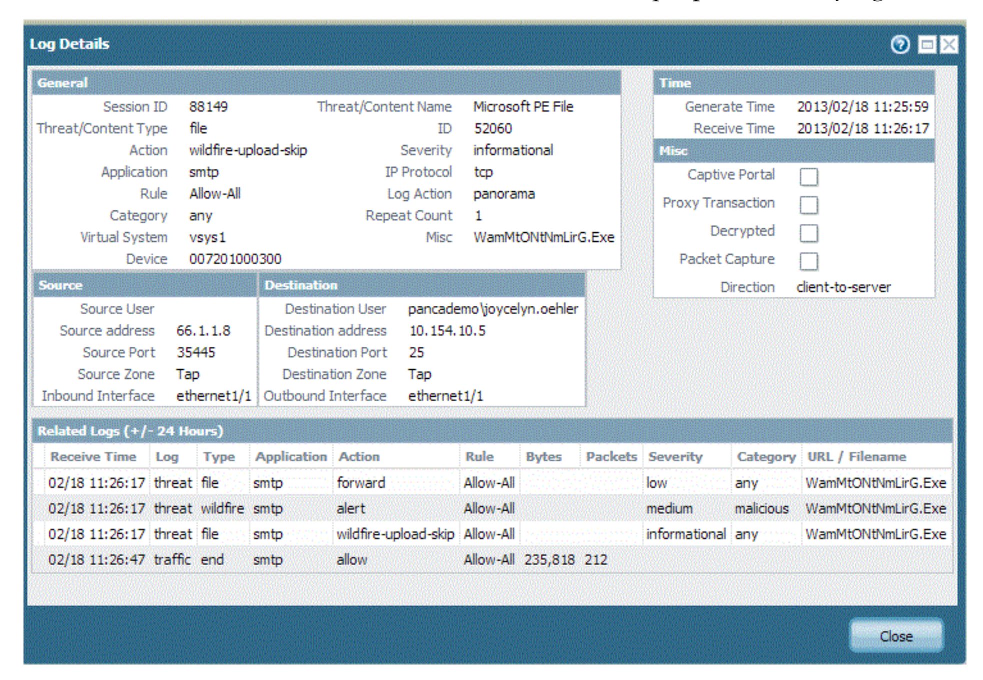
Además de los logs de amenaza, utilice la dirección IP de la víctima para filtrar los logs **WildFire Submissions (Presentaciones de WildFire)**. Los logs **WildFire Submissions (Presentaciones de WildFire)** contienen información sobre los archivos cargados en el servicio WildFire para su análisis. Como el spyware suele incrustarse encubiertamente, la revisión de los logs de WildFire le indicará si la víctima ha descargado recientemente un archivo sospechoso. El informe experto de WildFire muestra información de la URL de la que se obtuvo el archivo o .exe, así como el comportamiento del contenido. Le informa si el archivo es malintencionado, ha modificado las claves de registro, ha leído/escrito en archivos, ha creado nuevos archivos, ha abierto canales de comunicación de red, ha causado bloqueos de aplicaciones, ha generado procesos, ha descargado archivos o ha mostrado otro comportamiento malintencionado. Utilice esta información para determinar si desea bloquear la aplicación que provocó la infección (navegación web, SMTP, FTP), crear políticas de filtrado de URL más estrictas o restringir algunas aplicaciones o acciones como descargas de archivos a grupos de usuarios específicos.



Para acceder a los logs de WildFire desde Panorama necesita lo siguiente: una suscripción a WildFire, un perfil de bloqueo de archivos unido a una política de seguridad y el reenvío de logs de amenaza a Panorama.

Si WildFire determina que un archivo es malintencionado, se creará una nueva firma de antivirus en 24-48 horas y se pondrá a su disposición. Si tiene una suscripción a WildFire, la firma estará disponible en 30-60 minutos como parte de la próxima actualización de firma de WildFire. Tan pronto como el cortafuegos de próxima generación de Palo Alto Networks haya recibido una firma para ello, su configuración se ajustará para bloquear el software malintencionado, el archivo se bloqueará y la información del archivo bloqueado estará visible en sus logs de amenaza. Este proceso está fuertemente integrado para protegerle de esta amenaza y detiene la propagación del software malintencionado por su red.

El log de filtrado de datos (**Supervisar > Logs > Filtrado de datos**) es otro origen valioso para investigar la actividad de red malintencionada. Si bien puede revisar periódicamente los logs de todos los archivos sobre los que se le está alertando, también puede utilizar los logs para realizar un seguimiento de las transferencias de archivos y datos hacia o desde el usuario o la dirección IP de la víctima, así como verificar la dirección y el flujo del tráfico: de servidor a cliente o de cliente a servidor. Para recrear los eventos que precedieron y siguieron a un evento,



filtre los logs de la dirección IP de la víctima como destino y revise los logs en busca de la actividad de red.

Como Panorama agrega información de todos los dispositivos gestionados, presenta una buena descripción general de toda la actividad de su red. Otras herramientas visuales que puede utilizar para realizar un seguimiento del tráfico de su red son **Mapa de amenazas**, **Mapa de tráfico** y **Supervisor de amenazas**. El mapa de amenazas y el mapa de tráfico (**Supervisar > AppScope (Appscope) > Mapa de amenazas** o **Mapa de tráfico**) le permiten visualizar las regiones geográficas del tráfico de entrada y salida. Es de especial utilidad para visualizar actividad poco frecuente que podría indicar un posible ataque desde el exterior, como un ataque DDoS. Si, por ejemplo, no tiene muchas transacciones comerciales con Europa del Este y el mapa revela un nivel anómalo de tráfico con esa región, haga clic en el área correspondiente del mapa para iniciar y ver la información del ACC sobre las aplicaciones principales, información detallada de tráfico sobre el recuento de la sesión, los bytes enviados y recibidos, los orígenes y los destinos principales, los usuarios o las direcciones IP y la gravedad de las amenazas detectadas, si las hubiera. El supervisor de amenazas (**Supervisar > AppScope (Appscope) > Supervisor de amenazas**) muestra las diez amenazas principales de su red, o bien la lista de los atacantes principales o las víctimas principales de la red.

Con toda la información que ha descubierto, ahora puede hacerse una idea de cómo afectan las amenazas a su red (la escala del ataque, el origen, los host en peligro y el factor de riesgo) y evaluar que cambios, si los hubiera, debería realizar. Aquí tiene algunas sugerencias que considerar:

- Impedir ataques DDoS mejorando su perfil DoS para configurar un descarte aleatorio temprano o cancelar cookies SYN para inundaciones TCP. Considere establecer límites en el tráfico de ICMP y UDP. Evalúe las opciones que tiene a su disposición basándose en las tendencias y los patrones que ha observado en sus logs e implemente los cambios mediante plantillas de Panorama.

Cree una lista de bloqueos dinámicos [**Objects (Objetos) > Listas de bloqueos dinámicos**], para bloquear direcciones IP específicas que haya descubierto a partir de diversos orígenes de inteligencia: análisis de sus propios logs de amenaza, ataques DDoS desde direcciones IP específicas o una lista de bloqueo de IP de terceros.

La lista debe ser un archivo de texto y se debe encontrar en un servidor web. Mediante grupos de dispositivos de Panorama, introduzca el objeto en los cortafuegos gestionados para que puedan acceder al servidor web e importar la lista en una frecuencia definida. Tras crear un objeto de lista de bloqueos dinámicos, defina una política de seguridad que utilice el objeto de dirección en los campos de origen y destino para bloquear el tráfico desde o hacia la dirección IP, el rango o la subred definida. Este enfoque le permite bloquear a intrusos hasta que resuelva el problema y realizar cambios de política mayores para proteger su red.

- Determine si desea crear políticas compartidas o políticas de grupos de dispositivos para bloquear aplicaciones específicas que provocaron la infección (navegación web, SMTP, FTP), crear políticas de filtrado de URL más estrictas o restringir algunas aplicaciones o acciones como descargas de archivos a grupos de usuarios específicos.
- En Panorama, también puede cambiar al contexto de dispositivo y configurar el cortafuegos para informes de Botnet que identifiquen posibles host infectados de Botnet en la red.

5 Alta disponibilidad de Panorama

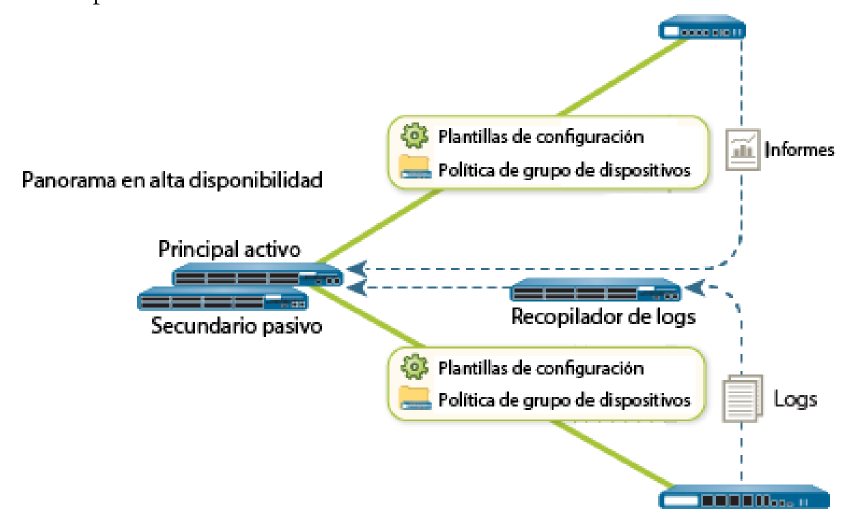


La alta disponibilidad (HA) de Panorama es una configuración en la que dos servidores de Panorama se sitúan en un grupo (clúster de dos dispositivos) para proporcionar redundancia en el caso de un fallo de red o del sistema. Panorama en HA proporciona continuidad en la tarea de administrar y supervisar los cortafuegos para asegurar la red de forma centralizada. Esta sección cubre los siguientes temas:

- ▲ Descripción general de la alta disponibilidad
- ▲ Configuración de un clúster en alta disponibilidad de Panorama
- ▲ Actualización de Panorama en alta disponibilidad

Descripción general de la alta disponibilidad

Panorama ofrece un panel centralizado para configurar, supervisar y realizar informes sobre los cortafuegos de Palo Alto Networks. Panorama en HA proporciona redundancia en las funciones de gestión central y creación de informes en su implementación.



Para configurar Panorama en HA, necesita un clúster de servidores de Panorama idénticos, con las siguientes características cada uno:

- **El mismo factor de forma**: ambos deben ser dispositivos basados en hardware (dispositivos M-100) o virtuales. Para la HA, los dispositivos M-100 deben estar en modo Panorama; HA no es compatible con un clúster de dispositivos M-100 configurados como recopiladores de logs.
- **La misma versión del sistema operativo de Panorama**: deben ejecutar la misma versión de Panorama para sincronizar la información de configuración y mantener la paridad para una conmutación por error sin problemas.
- **El mismo conjunto de licencias**: debe adquirir e instalar la misma licencia de capacidad de gestión del dispositivo para cada instancia de Panorama.
- **(Solo para dispositivo virtual de Panorama) Número de serie único**: debe contar con un número de serie único para cada dispositivo virtual de Panorama; si el número de serie está duplicado, ambas instancias de Panorama pasarán al modo de suspensión hasta que resuelva el problema.

Los servidores de Panorama en una configuración de HA son peers y cada uno de ellos se puede utilizar para gestionar de forma centralizada los dispositivos con algunas excepciones. Los pares de HA utilizan el puerto de gestión para sincronizar los elementos de configuración transferidos a los dispositivos gestionados y mantener la información de estado. Normalmente, los pares de HA de Panorama se ubican geográficamente en diferentes sitios, por lo que debe asegurase de que la dirección IP del puerto de gestión asignada a cada peer es enrutable a través de la red. La conectividad de HA utiliza el puerto TCP 28 con el cifrado habilitado y 28769 cuando el cifrado no está habilitado.

Cada dispositivo del clúster en HA se asigna a un valor de *prioridad*. El valor de prioridad de *principal* o *secundario* determina qué peer de Panorama podrá ser seleccionado para ser el punto principal de administración y gestión de logs. El peer establecido como *principal* asume el estado *activo* y el *secundario* el *pasivo*. El dispositivo activo gestiona todos los cambios de configuración y los transfiere a los cortafuegos gestionados; el dispositivo pasivo no puede realizar ningún cambio de configuración ni transferir configuración a los dispositivos gestionados. Sin embargo, cualquier peer se puede utilizar para ejecutar informes o realizar consultas de log.

El peer pasivo se sincroniza y se prepara para la transición al estado activo, si se produjera un fallo en la ruta, enlace, sistema o red en el dispositivo activo.

Activadores de conmutación por error

Cuando se produce un fallo en el dispositivo activo y el dispositivo pasivo toma el control de la tarea de gestionar los cortafuegos, el evento se denomina "conmutación por error". Una conmutación por error se activa cuando falla una métrica supervisada en el dispositivo activo. Este fallo pasa el Panorama principal de *activo-principal* a *pasivo-principal* y el Panorama secundario se convierte en *activo-secundario*.

Las condiciones que activan una conmutación por error son las siguientes:

- Los peers de Panorama no se pueden comunicar entre sí y el peer activo no responde a los sondeos de estado; la métrica utilizada es Sondeos de heartbeat y mensajes de saludo.

  Cuando los peers de Panorama no se pueden comunicar entre sí, el peer activo supervisa si los dispositivos siguen conectados a él antes de que se active una conmutación por error. Esta comprobación ayuda a evitar una conmutación por error y a que no se produzca una situación de síndrome de cerebro dividido, donde los dos peers de Panorama pasan a estar activos.

- No se puede llegar a uno o varios destinos (direcciones IP) especificados en el peer activo; la métrica utilizada es Supervisión de rutas.

Además de los activadores de conmutación por error enumerados anteriormente, también se produce una conmutación por error cuando el administrador coloca el dispositivo en un estado suspendido o si se produce una *preferencia*. Esta función se refiere a la preferencia por la instancia principal de Panorama a la hora de reanudar la función activa después de recuperarse de un fallo (suspensión iniciada por el usuario). De forma predeterminada, la función de preferencia está habilitada; cuando la instancia de Panorama principal se recupera de un fallo y vuelve a estar disponible, la instancia de Panorama secundaria deja el control y vuelve al estado pasivo. Cuando se produce una preferencia, el evento se registra en el log del sistema.

Si está creando un log en un almacén de datos de NFS, no deshabilite la función de preferencia, ya que permite al peer principal (montado en el NFS) reanudar la función activa y escribir en el almacén de datos de NFS. Para otras implementaciones, la función de preferencia solo es necesaria si desea asegurarse de que un dispositivo específico es el dispositivo activo preferido.

Sondeos de heartbeat y mensajes de saludo

Los peers de HA utilizan mensajes de saludo y heartbeats para comprobar que el peer responde y está operativo. Los mensajes de saludo se envían desde un peer al otro en el *intervalo de saludo* configurado para verificar el estado del dispositivo. El heartbeat es un ping ICMP para el peer de HA y el peer responde al ping para establecer que los dispositivos están conectados y responden. De manera predeterminada, el intervalo para el heartbeat es de 1000 milisegundos y 8000 milisegundos para los mensajes de saludo.

Supervisión de rutas

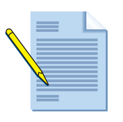
La supervisión de rutas comprueba la conectividad de la red y el estado del enlace de una dirección IP específica. El peer activo utiliza pings ICMP para comprobar que se pueden alcanzar una o varias direcciones IP de destino. Puede, por ejemplo, supervisar la disponibilidad de dispositivos de red interconectados como un enrutador o un conmutador, la conectividad a un servidor o cualquier otro dispositivo vital que se encuentre en el flujo del tráfico. Asegúrese de que no sea probable que el nodo/dispositivo configurado para la supervisión no responda, especialmente cuando tenga una carga inferior, ya que esto podría provocar un fallo de supervisión de rutas y activar una conmutación por error.

El intervalo de ping predeterminado es de 5000 ms. Se considera que no se puede llegar a una dirección IP cuando fallan 3 pings consecutivos (el valor predeterminado) y se activa un fallo de dispositivo cuando no se puede llegar a alguna o todas las direcciones IP supervisadas. De forma predeterminada, si no se puede alcanzar alguna de las direcciones IP, el estado de HA pasa a ser *no funcional*.

Consideraciones sobre el registro en HA

El establecimiento de una configuración de HA en Panorama proporciona redundancia para la recopilación de logs. Debido a que los dispositivos gestionados están conectados a ambos peers de Panorama en la SSL, cuando se produce un cambio de estado, las instancias de Panorama envían un mensaje a los dispositivos gestionados. Se informa a los dispositivos sobre el estado de HA de Panorama y estos pueden enviar los logs correspondientes.

Las opciones de registro en la instancia de Panorama basada en hardware y en el dispositivo virtual de Panorama son diferentes.



By default, when the managed devices cannot connect to Panorama (M-100 appliance and the Panorama virtual appliance), they buffer the logs; when the connection is restored, they resume sending logs from where it was last left off.

Registro de una conmutación por error en un dispositivo virtual de Panorama

En el dispositivo virtual de Panorama, tiene las siguientes opciones:

- **Registro en un disco virtual:** De forma predeterminada, los dispositivos gestionados envían logs a ambos peers del clúster en HA; los logs se envían como secuencias de logs independientes a cada peer de HA de Panorama. Si un peer no está disponible, de forma predeterminada, los dispositivos gestionados guardan en el búfer los logs y cuando el peer se vuelve a conectar, continúan enviado logs donde lo dejaron la última vez (sujeto a la capacidad de almacenamiento del disco y a la duración de la desconexión).

  El registro en un disco virtual proporciona redundancia en el proceso, aunque la capacidad de almacenamiento de log está limitada a un máximo de 2 TB.



The option to forward logs to the active peer only is configurable (See Modificación de los valores predeterminados de almacenamiento en búfer y reenvío de logs, to modify this option). Sin embargo, la agregación de logs no es compatible en todo el clúster en HA. De esta forma, si está registrando en un disco virtual o local, para la supervisión y la creación de informes debe consultar al peer de Panorama que recopila los logs de los dispositivos gestionados.

- **Registro en un sistema de archivos de red (NFS):** Cuando se ha configurado el uso de un NFS, solo el dispositivo *activo-principal* se monta en la partición de logs basados en NFS y puede recibir logs. En la conmutación por error, el dispositivo principal pasa al estado *pasivo-principal*. En este estado, hasta que se produzca la preferencia, la instancia activa-secundaria de Panorama gestiona los dispositivos, pero no recibe logs y no puede escribir en el NFS. Para permitir que el peer activo-secundario se registre en el NFS, debe cambiarlo a principal manualmente de forma que pueda montarse en la partición del NFS. Para obtener instrucciones, consulte Cambio de prioridad para reanudar los logs en NFS.

Registro de logs en un dispositivo M-100

Si utiliza un par de dispositivos M-100 (debe encontrarse en modo Panorama), los dispositivos gestionados pueden enviar logs solamente a un peer del clúster en HA, activo o pasivo.

Unlike the virtual Panorama deployment, you cannot configure the devices to send logs to both peers, however, the RAID-enabled disks on the M-100 appliance protect against disk failure and loss of logs.

Si tiene una recopilación de logs distribuida establecida a cuyo recopilador de logs especializado estén enviando logs los dispositivos gestionados, los peers de Panorama en HA consultarán todos los recopiladores de logs gestionados para encontrar información del log agregado.

Prioridad y conmutación por error

Cuando se produce una conmutación por error, solo cambia el estado (activo o pasivo) del dispositivo; la prioridad (principal o secundaria) no lo hace. Por ejemplo, cuando falla el peer principal, su estado cambia de *activo-principal* a *pasivo-principal*.

Un peer en estado activo-secundario puede realizar todas las funciones con dos excepciones:

- No puede gestionar las funciones de implementación del dispositivo como actualizaciones de licencia o de software en los cortafuegos gestionados.
- No puede registrar en un NFS hasta que no cambie manualmente su prioridad a principal. (Solo dispositivo virtual de Panorama)

En la siguiente tabla se indican las capacidades de Panorama basadas en la configuración de su estado y prioridad:

Capacidad	activa-principal	pasiva-principal pasiva-secundaria	activa-secundaria
Cambiar contexto de dispositivo	🟩	🟩	🟩
Realizar informes distribuidos	🟩	🟩	🟩
Gestionar política compartida	🟩	🟥	🟩
Iniciar sesión en un disco local	🟩	🟩 (Optional on the Panorama virtual appliance only)	🟩 (Optional on the Panorama virtual appliance only)
Iniciar sesión en una partición NFS (Solo dispositivo virtual de Panorama)	🟩	🟥	🟥
Implementar software y licencias	🟩	🟥	🟥
Exportar configuración de Panorama	🟩	🟩	🟩

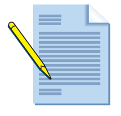
¿Qué configuración no está sincronizada entre los peers de HA?

Los peers de HA de Panorama sincronizan la configuración en ejecución cada vez que compila cambios en el peer activo de Panorama. La configuración candidata se sincroniza entre los peers cada vez que guarda la configuración en el peer activo o justo antes de que se produzca una conmutación por error.

La configuración común entre los clústeres, como los objetos y políticas compartidos, los objetos de grupo de dispositivos y las políticas, la configuración de plantilla y la configuración de acceso administrativo se sincronizan entre los peers de HA de Panorama.

La configuración que no se sincroniza es aquella específica de cada peer, como la siguiente:

- Configuración de HA de Panorama: ajuste de prioridad, dirección IP del peer, grupos de supervisión de ruta y direcciones IP
- Configuración de Panorama: dirección IP del puerto de gestión, configuración FQDN, titular de inicio de sesión, servidor de NTP, zona horaria, ubicación geográfica, servidor DNS, direcciones IP permitidas para acceder a Panorama y configuración del sistema SNMP
- Configuración de partición NFS y toda la asignación de cuota de disco para los logs
- Asignación de cuota de disco para los diferentes tipos de logs y bases de datos en el almacenamiento local de Panorama (SSD)



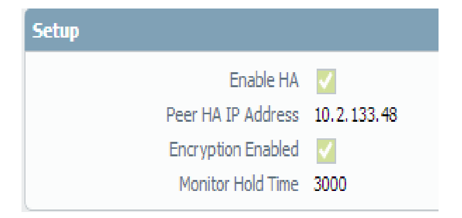
Si utiliza una clave maestra para cifrar las claves privadas usadas en Panorama, se debe utilizar la misma clave maestra para cifrar las claves privadas y los certificados en ambos peers del clúster en HA. Si las claves maestras son diferentes, la configuración de HA no se sincronizará entre peers.

Configuración de un clúster en alta disponibilidad de Panorama

Asegúrese de revisar los requisitos de la sección Descripción general de la alta disponibilidad antes de configurar un clúster en HA de Panorama:

- Configuración de alta disponibilidad en Panorama
- Verificación de conmutación por error
- (Solo dispositivo virtual de Panorama) Cambio de prioridad para reanudar los logs en NFS

Configuración de alta disponibilidad en Panorama

CONEXIÓN Y CONFIGURACIÓN DE LOS DISPOSITIVOS		
Paso 1	Configure la conectividad entre los puertos MGT en los peers de HA.	Los peers de Panorama se comunican entre sí usando el puerto MGT. Asegúrese de que las direcciones IP que asigna al puerto MGT en los servidores Panorama del clúster en HA son enrutables y que los peers se pueden comunica entre sí a través de la red. Para configurar el puerto MGT, consulte el Capítulo 2, Configuración de Panorama.
▲ Seleccione un dispositivo del clúster y realice estas tareas:		
Paso 2	Habilite la HA y el cifrado para la conexión de HA.  	1. Seleccione la pestaña **Panorama > Alta disponibilidad**. Edite la sección **Configuración**. 2. Seleccione **Habilitar HA**. 3. Introduzca la dirección IP asignada al dispositivo peer en **Dirección IP de HA del peer**. 4. (Opcional) Para habilitar el cifrado, seleccione **Cifrado habilitado** y realice las siguientes tareas: a Seleccione **Panorama > Gestión de certificados > Certificados**. b Seleccione **Exportar clave de HA**. Guarde la clave de HA en una ubicación de red a la que pueda acceder el dispositivo peer. c En el dispositivo peer, vaya a **Panorama > Gestión de certificados > Certificados** y seleccione **Importar clave de HA** para llegar a la ubicación en la que ha guardado la clave e impórtela.

CONEXIÓN Y CONFIGURACIÓN DE LOS DISPOSITIVOS (CONTINUACIÓN)

Paso 3 Establezca la prioridad.

1. En **Panorama > Alta disponibilidad**, edite la sección **Configuración de elección**.
2. Defina **Prioridad de dispositivo** como **Principal** o **Secundario**. Asegúrese de establecer un peer como principal y el otro como secundario.

Nota Si ambos peers tienen el mismo ajuste de prioridad, el peer con el número de serie más alto quedará suspendido.

3. Defina el comportamiento como **Preferente**. De forma predeterminada, la función de preferencia está habilitada. La selección de preferencia (habilitada o deshabilitada) debe ser igual en ambos peers.

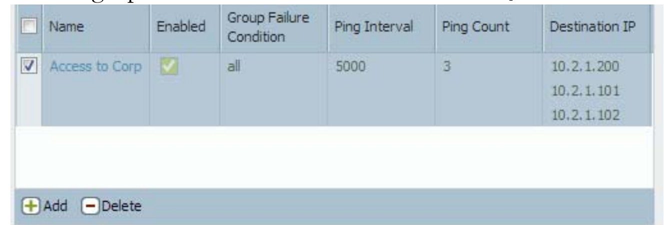
Nota Si utiliza un NFS para los logs y ha desactivado la preferencia, para reanudar la creación de logs en el NFS, consulte Cambio de prioridad para reanudar los logs en NFS.

Paso 4 Para configurar la supervisión de ruta, defina uno o varios grupos de ruta.

El grupo de rutas indica las direcciones IP de destino (nodos) en los que Panorama debe hacer ping para comprobar la conectividad de la red.

1. Seleccione **Panorama > Alta disponibilidad** y haga clic en **Añadir** en la sección grupo de rutas .
2. Introduzca un **nombre** para el grupo de rutas.
3. Haga clic en **Añadir** e introduzca las direcciones IP de destino que le gustaría supervisar.
4. En **Condición de fallo**, seleccione **Todos** o **Cualquiera**— para este grupo.
   - La condición de fallo **Cualquiera** activa un supervisor de enlaces en caso de que no se pueda acceder a alguna de las direcciones IP.
   - **Todos** activa un supervisor de enlace solo cuando no se puede acceder a ninguna de las direcciones IP .

   El grupo de rutas se añade a la sección **Grupo de rutas.**



	Name	Enabled	Group Failure Condition	Ping Interval	Ping Count	Destination IP
☑	Access to Corp	✓	all	5000	3	10.2.1.200 10.2.1.101 10.2.1.102

5. Repita los pasos del 1 al 4 para agregar más grupos de rutas que incluyan los nodos que desea supervisar.

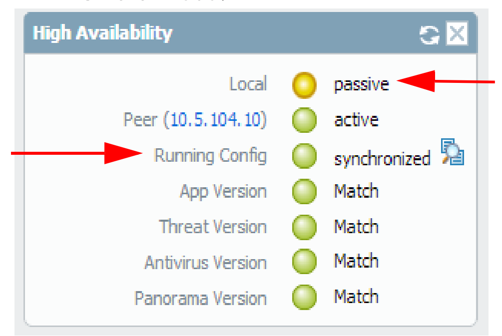
Paso 5 (Opcional) Seleccione la condición de fallo para la supervisión de rutas en Panorama.

Seleccione **Panorama > Alta disponibilidad** y seleccione una **condición de fallo** en la sección Supervisión de rutas.

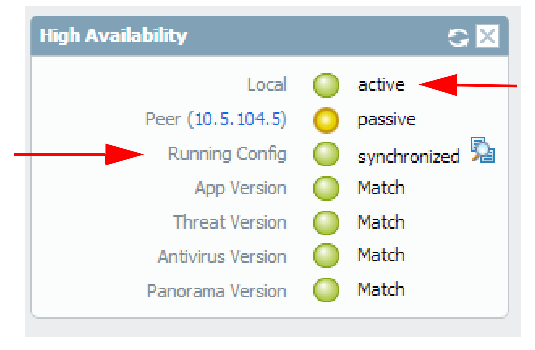
- La condición de fallo **Todos** activa una conmutación por error solo cuando fallan todos los grupos de rutas supervisados.
- La configuración predeterminada es **Cualquiera**; se activa una conmutación por error cuando falla algún grupo de rutas.

CONEXIÓN Y CONFIGURACIÓN DE LOS DISPOSITIVOS (CONTINUACIÓN)		
Paso 6	Guarde los cambios de configuración.	Haga clic en **Compilar**, seleccione **Panorama** en la opción **Compilar tipo** y haga clic en **ACEPTAR**.
Paso 7	Configure el otro peer de Panorama.	Repita del Paso 2 al Paso 6 en el otro peer del clúster en HA.
Paso 8	Compruebe que los servidores de Panorama están en configurados en clúster en HA.	Después de terminar de configurar ambos servidores Panorama para HA: 1. Acceda a **Panel** en cada instancia de Panorama y consulte el widget **Alta disponibilidad**. 2. Confirme que los servidores de Panorama se configuran en clúster y sincronizan, como se muestra a continuación:

En la instancia pasiva de Panorama: El estado del peer local debe aparece como **pasivo** y la configuración debe estar **sincronizada**.



En la instancia activa de Panorama: El estado del peer local debe aparecer como **activo** y la configuración debe estar **sincronizada**.

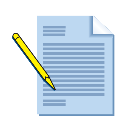


Verificación de conmutación por error

Para comprobar que su configuración de HA funciona correctamente, active una conmutación por error manual y verifique que el peer cambia de estado correctamente.

VERIFICACIÓN DE CONMUTACIÓN POR ERROR		
Paso 1	Inicie sesión en el peer activo de Panorama.	Puede verificar el estado del servidor de Panorama en la esquina inferior derecha de la interfaz web.
Paso 2	Suspenda el peer activo de Panorama.	Seleccione **Panorama > Alta disponibilidad** y, a continuación, haga clic en el enlace para **suspender Panorama local** en la sección Comandos de operación.
Paso 3	Compruebe que el peer de Panorama pasivo ha pasado a activo.	En el **Panel** de Panorama, compruebe que el estado del servidor pasivo cambia a **activo** en el widget **Alta disponibilidad**. De igual forma, compruebe que el estado del peer ha cambiado a suspendido.
Paso 4	Restaure el peer suspendido a un estado funcional. Espere un par de minutos y, a continuación, verifique que se ha producido la preferencia, si se ha habilitado.	En la instancia de Panorama previamente suspendida: 1. En la sección Comandos de operación de la pestaña **Dispositivo > Alta disponibilidad**, haga clic en el enlace **Make local Panorama functional (Hacer Panorama local funcional)**. 2. En el widget **Alta disponibilidad** del **Panel**, confirme que esta instancia (local) de Panorama ha pasado como el peer activo y que el otro peer está ahora en estado pasivo.

Cambio de prioridad para reanudar los logs en NFS



Solo el dispositivo virtual de Panorama es compatible con un mecanismo de log basado en NFS (Network File Share).

Cuando un clúster en HA de Panorama se configura para utilizar un mecanismo de log basado en NFS, solo el peer *principal* de Panorama se monta en la partición de logs basada en NFS y puede escribir en el NFS. Cuando se produce una conmutación por error y el Panorama pasivo se vuelve activo, su estado es activo-secundario. Aunque un peer secundario de Panorama puede gestionar activamente los dispositivos, no puede recibir logs ni escribir en el NFS porque no posee la partición NFS. Cuando el dispositivo gestionado no puede reenviar logs al peer *principal* de Panorama, los logs se escriben en el disco local de cada dispositivo. Los dispositivos mantienen un puntero para el último conjunto de entradas de logs reenviados a Panorama, de forma que cuando el Panorama *pasivo-principal* se vuelve disponible otra vez, puede seguir reenviándole logs.

Utilice las instrucciones de esta sección para cambiar manualmente la prioridad en el peer *activo-secundario* de Panorama para que pueda empezar a crear logs en la partición NFS. Los casos típicos en los que debería tener que activar este cambio son los siguientes:

- Cuando la función de preferencia está deshabilitada. De forma predeterminada, la preferencia está habilitada en Panorama y el peer principal se reanuda como activo cuando vuelve a estar disponible. Cuando la preferencia está desactivada, debe cambiar la prioridad en el peer secundario a *principal* de forma que puedan montar la partición NFS, recibir logs de los dispositivos gestionados y escribir en la partición NFS.
- La instancia activa de Panorama falla y no puede recuperarse del falo a corto plazo.
- Si no cambia la prioridad y cuando se alcance la capacidad máxima de almacenamiento de logs, los logs más antiguos se sobrescriben para seguir permitiendo la creación de logs en el disco local. Esta situación puede hacer que se pierdan logs.

CAMBIO DE PRIORIDAD EN PANORAMA		
Paso 1	Desconecte la instancia pasiva-principal actual de Panorama.	Seleccione **Panorama > Configuración > Operaciones** y haga clic en **Shutdown Panorama (Cerrar Panorama)** en la sección Operaciones de dispositivo.
Paso 2	Cambie la prioridad en la instancia activa-secundaria de Panorama.	1. Seleccione **Panorama > Alta disponibilidad**. 2. Edite la sección Configuración de elección para cambiar la **prioridad** a **Principal**
Paso 3	Guarde sus cambios de configuración.	Haga clic en **Compilar** y seleccione **Panorama** en la opción **Compilar tipo**. Al compilar, se le pedirá reiniciar; lo reinicie todavía.
Paso 4	Inicio de sesión en la CLI y cambie la propiedad de la partición NFS a este peer.	En la CLI, introduzca el siguiente comando: `request high-availability convert-to-primary`
Paso 5	Reinicie Panorama.	Seleccione **Panorama > Configuración > Operaciones** y haga clic en **Reiniciar Panorama** en la sección Operaciones de dispositivo. Cuando Panorama se reinicia, montará dinámicamente el NFS. Como el peer *activo-principal*, este Panorama puede escribir ahora en NFS.
Paso 6	Conecte el peer de Panorama que desconectó en el paso 1. Este peer pasará ahora al estado pasivo-secundario.	

Actualización de Panorama en alta disponibilidad

Para garantizar una conmutación por error sin problemas, los peers principal y secundario de Panorama en un clúster en HA deben tener la misma versión de Panorama y las mismas versiones de las bases de datos de aplicaciones y amenazas.

En el siguiente ejemplo se muestra cómo actualizar un clúster en HA con un peer activo-principal denominado Principal_A y el peer pasivo-secundario denominado Secundario_B.

ACTUALIZACIÓN DE PANORAMA		
Paso 1	Actualice la versión de software de Panorama en Secundario_B, el peer pasivo-secundario.	Para obtener instrucciones sobre la actualización, consulte Instalación de las actualizaciones de contenido y software de Panorama. Al actualizar este Panorama, se pasa a un estado no funcional porque la versión del sistema operativo no coincide con la de su peer.
Paso 2	Suspenda el Principal_A para activar una conmutación por error.	En la pestaña **Panorama > Alta disponibilidad** en el Principal_A: 1. Haga clic en el enlace **Suspend local Panorama (Suspender Panorama local)** en la sección **Comandos de operación** para suspender este peer. 2. Compruebe que el estado aparece como suspendido; el estado aparece en la esquina inferior derecha de la interfaz web. Si pasa Principal_A a modo suspendido, se activa una conmutación por error y Secundario_B pasa al estado activo-secundario.
Paso 3	Actualice la versión de software de Panorama de Principal_A.	Para obtener instrucciones sobre la actualización, consulte Instalación de las actualizaciones de contenido y software de Panorama. Al reiniciar, Principal_A cambia primero al estado pasivo-principal. A continuación, como la preferencia está habilitada de forma predeterminada, Principal_A cambiará automáticamente al estado activo-principal y Secundario_B volverá al estado pasivo-secundario. Si ha deshabilitado la función de preferencia, consulte Restauración del servidor principal al estado activo para restaurar Principal_A al estado activo.
Paso 4	Compruebe que la versión de software de Panorama y otras versiones de las bases de datos de contenido son iguales en ambos peers.	En el **Panel** de cada uno de los peers de Panorama, compruebe que la versión de software de Panorama, la versión de amenazas y las versiones de la aplicación **coinciden** y que la configuración en ejecución está **sincronizada** con el peer.

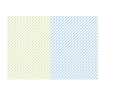
Restauración del servidor principal al estado activo

De forma predeterminada, la función de preferencia de Panorama permite a la instancia principal de Panorama continuar funcionando como el peer activo tan pronto como está disponible. Sin embargo, si la función de preferencia está deshabilitada, la única manera de que la instancia principal de Panorama pase a estar activa tras recuperarse de un fallo, un estado no funcional o suspendido es suspendiendo el peer secundario de Panorama.

Antes de que la instancia activa-secundaria de Panorama pase a un estado suspendido, transfiere la configuración candidata al dispositivo pasivo de forma que todos los cambios de configuración no compilados se guardan y se puede acceder a ellos a través del otro peer.

SUSPENSIÓN DE PANORAMA	
Paso 1 Suspenda Panorama.	1. Inicie la sesión en el peer de Panorama que desea que pase al estado de suspensión. 2. Seleccione **Panorama > Alta disponibilidad** y haga clic en el enlace **Suspend local Panorama (Suspender Panorama local)** en la sección Comandos de operación.
Paso 2 Compruebe que el estado indica que el dispositivo se ha suspendido bajo la solicitud del usuario.	En el widget **Alta disponibilidad** del **Panel**, compruebe que el estado aparece como suspendido. Cuando se suspende un peer, se activa una conmutación por error y la otra instancia de Panorama cambia a peer activo.

RESTAURACIÓN DE PANORAMA A UN ESTADO FUNCIONAL	
Para restaurar la instancia suspendida de Panorama a un estado funcional.	1. Haga clic en el enlace **Make local Panorama functional (Hacer Panorama local funcional)** en la sección Comandos de operación de la pestaña **Panorama > Alta disponibilidad**. 2. En el widget **Alta disponibilidad** del **Panel**, confirme que el dispositivo ha pasado al estado activo o pasivo.



6 Administración de Panorama

En esta sección se describe cómo administrar y mantener Panorama. Incluye los siguientes temas:

- Gestión de las copias de seguridad de la configuración
- Comparación de cambios en la configuración
- Restricción de acceso a los cambios de configuración
- Adición de logotipos personalizados
- Visualización del historial de finalización de tareas
- Reasignación de cuotas de almacenamiento de logs
- Supervisión de Panorama
- Reinicio o cierre de Panorama
- Generación de archivos de diagnóstico
- Configuración de perfiles de contraseña y complejidad de contraseña
- Sustitución del disco virtual en un dispositivo virtual de Panorama



Para obtener instrucciones sobre cómo completar la configuración inicial, incluida la definición de los ajustes de acceso a la red, la creación de licencias, la actualización de la versión del software Panorama y la configuración del acceso administrativo a Panorama, consulte el Capítulo 2, Configuración de Panorama.

Gestión de las copias de seguridad de la configuración

Una copia de seguridad de la configuración es una instantánea de la configuración del sistema. En caso de fallo del sistema o error en la configuración, una copia de seguridad de la configuración le permite restaurar Panorama a una versión de la configuración guardada anteriormente. En Panorama, puede gestionar las copias de seguridad de la configuración de los cortafuegos gestionados y de Panorama:

- **Gestión de copias de seguridad de configuración de los dispositivos gestionados**: Panorama guarda automáticamente todos los cambios de configuración que se producen en un cortafuegos gestionado que ejecute la versión 5.0 o posterior de PAN-OS. De forma predeterminada, Panorama almacena hasta 100 versiones de cada dispositivo. Este valor es configurable.

- **Gestión de las copias de seguridad de configuración de Panorama**: Puede exportar manualmente la configuración en ejecución de Panorama, según sea necesario.

- **Exportación de un paquete de archivos de configuración**: Además de la configuración que se ejecuta en él mismo, Panorama guarda una copia de seguridad de la configuración que se ejecuta en todos los dispositivos gestionados. Puede generar un paquete gzip de la versión más reciente de la copia de seguridad de la configuración de Panorama y de todos los dispositivos gestionados a demanda o programando una exportación mediante la función **Exportación de configuración programada**. Se puede programar el envío diario del paquete a un servidor FTP o a un servidor Secure Copy (SCP); los archivos del paquete están en formato XML y cada nombre de archivo hace referencia al número de serie del dispositivo para que la identificación sea sencilla.

Puede realizar las siguientes tareas para gestionar las copias de seguridad de la configuración:

▲ Programación de la exportación de los archivos de configuración

▲ Gestión de las copias de seguridad de configuración de Panorama

▲ Configuración del número de copias de seguridad almacenadas en Panorama

▲ Carga de una copia de seguridad de configuración en un dispositivo gestionado

Programación de la exportación de los archivos de configuración

Utilice estas instrucciones para programar la exportación del paquete de archivos de configuración que contiene la copia de seguridad de la configuración en ejecución de Panorama y de los dispositivos gestionados diariamente a una hora concreta. Son necesarios privilegios de superusuario para configurar la exportación.

PROGRAMACIÓN DE LA EXPORTACIÓN DE LOS ARCHIVOS DE CONFIGURACIÓN DIARIAMENTE A UNA HORA CONCRETA
1. Seleccione **Panorama > Exportación de configuración programada**.
2. Haga clic en **Añadir** e introduzca un **nombre** y una **descripción** para el proceso de exportación del archivo.
3. Seleccione **Habilitar** para permitir la exportación del archivo de configuración.
4. Introduzca una hora o seleccione una en la lista desplegable para que se realice una exportación diaria de los archivos de configuración. Se utiliza un reloj de 24 horas.
5. Seleccione el protocolo.
6. Introduzca los detalles para acceder al servidor. Proporcione el nombre del host o la dirección IP, el puerto o la ruta para cargar el archivo y las credenciales de autenticación.
7. (Solo SCP) Haga clic en **Conexión de servidor SCP de prueba**. Para activar la transferencia segura de los datos, debe verificar y aceptar la clave de host del servidor SCP. La conexión no se establece hasta que acepte la clave de host.
Si Panorama puede conectarse correctamente al servidor SCP, se crea y carga el archivo de prueba denominado **ssh-export-test.txt**.
8. Guarde los cambios. Haga clic en **Compilar**, seleccione **Panorama** como **Compilar tipo** y haga clic en **ACEPTAR**.

Gestión de las copias de seguridad de configuración de Panorama

Use estas instrucciones para validar, revertir, guardar, cargar, exportar o importar una versión de configuración de Panorama.

GESTIÓN DE COPIAS DE SEGURIDAD: VALIDAR, REVERTIR, GUARDAR, CARGAR, EXPORTAR O IMPORTAR

1. Seleccione **Panorama > Configuración > Operaciones**.
2. En la sección Gestión de configuración, elija una de las siguientes opciones:
   - **Validar configuración de Panorama de candidato**: comprueba que la configuración candidata no presenta errores; la validación del archivo de configuración le permite resolver errores antes de compilar los cambios.
   - **Volver a la última configuración guardada Panorama**: sobrescribe la configuración candidata actual y restaura la última configuración candidata guardada del disco.
   - **Volver a la configuración en ejecución Panorama**: revierte todos los cambios guardados en la configuración candidata; le permite deshacer de forma efectiva todos los cambios de configuración realizados desde la última compilación.
   - **Guardar la configuración Panorama en ejecución con nombre**: guarda la configuración candidata en un archivo. Introduzca un nombre de archivo o seleccione un archivo existente para sobrescribirlo. Tenga en cuenta que el archivo de configuración activa actual (running-config.xml) no puede sobrescribirse.
   - **Guardar la configuración candidata Panorama**: guarda la configuración candidata en un disco; es lo mismo que utilizar el enlace **Guardar** de la parte superior de la página para guardar los cambios en el archivo de configuración candidata.
   - **Cargar versión de la configuración Panorama**: carga un archivo de configuración de una lista de versiones compiladas anteriormente.
   - **Cargar configuración con nombre Panorama**: carga una configuración candidata seleccionada; puede seleccionar una configuración importada o cargada anteriormente. La configuración candidata actual se sobrescribirá.
   - **Exportar copia de configuración con nombre Panorama**: exporta la configuración activa (running-config.xml) o una configuración guardada o importada anteriormente. Seleccione el archivo de configuración que debe exportarse. Puede abrir el archivo y/o guardarlo en cualquier ubicación de red.
   - **Exportar versión de la configuración Panorama**: exporta una versión compilada anteriormente del archivo de configuración. Seleccione la versión que se debe exportar.
   - **Exportar lote de configuración de dispositivos y Panorama**: esta opción se utiliza para generar manualmente y exportar la versión más reciente de la copia de seguridad de configuración de Panorama y de los dispositivos gestionados. Para automatizar el proceso de crear y exportar el lote de configuración diariamente a un servidor SCP o FTP, consulte Programación de la exportación de los archivos de configuración.
   - **Importar configuración Panorama por nombre**: importa un archivo de configuración exportado anteriormente. Haga clic en **Examinar** para encontrar el archivo guardado y hacer clic en **ACEPTAR** para importar.

Configuración del número de copias de seguridad almacenadas en Panorama

Especifique el número de copias de seguridad de Panorama que se almacenan.

CONFIGURACIÓN DEL NÚMERO DE COPIAS DE SEGURIDAD ALMACENADAS EN PANORAMA
1. Seleccione **Panorama > Configuración > Gestión** y haga clic en el botón Editar en la sección Configuración de logs e informes. Number of Versions for Config Audit 100 Number of Versions for Config Backups 100
2. Introduzca un valor entre 1 y 1048576. El valor predeterminado es de 100.
3. Guarde los cambios. Haga clic en **Compilar**, seleccione **Panorama** como **Compilar tipo** y haga clic en **ACEPTAR**.

Carga de una copia de seguridad de configuración en un dispositivo gestionado

Utilice Panorama para cargar una copia de seguridad de configuración en un dispositivo gestionado Puede elegir volver a una configuración anteriormente guardada o compilada en el dispositivo. Panorama transfiere la versión seleccionada al dispositivo gestionado y se sobrescribe la configuración candidata actual en el dispositivo.

CARGA DE UNA COPIA DE SEGURIDAD DE CONFIGURACIÓN EN UN DISPOSITIVO GESTIONADO
1. Seleccione **Panorama > Dispositivos gestionados**.
2. Seleccione el enlace **Gestionar...** en la columna **Copias de seguridad**.
3. Seleccione en **Configuraciones guardadas** o **Configuraciones compiladas**. • Haga clic en el enlace de la columna **Versión** para ver el contenido de la versión seleccionada. • Haga clic en **Cargar** para cargar una versión de configuración seleccionada.
4. Guarde los cambios. Haga clic en **Compilar** y seleccione **Panorama** como **Compilar tipo**.

Comparación de cambios en la configuración

Para comparar los cambios en la configuración en Panorama, puede seleccionar cualquier par de conjuntos de archivos de configuración: la configuración candidata, la configuración en ejecución o cualquier otra versión de la configuración que se haya guardado o compilado anteriormente en Panorama. La comparación de los archivos le permite:

- Obtener una vista previa de los cambios en la configuración antes de compilarlos en Panorama. Puede, por ejemplo, obtener una vista previa de los cambios entre la configuración candidata y la configuración en ejecución. Se recomienda seleccionar la versión más antigua en el panel izquierdo y la más reciente en el derecho, para comparar e identificar las modificaciones fácilmente.
- Realice una *auditoría de configuraciones* para revisar y comparar los cambios entre dos conjuntos de archivos de configuración.

COMPARACIÓN DE CAMBIOS EN LA CONFIGURACIÓN	
• Vea y compare los archivos de configuración. Se resaltan los cambios con el fin de comparar versiones con facilidad: Added Modified Deleted	1. Seleccione **Panorama > Auditoría de configuraciones**. 2. En cada menú desplegable, seleccione una configuración para la comparación. 3. Seleccione el número de líneas que desee incluir para el **contexto** y haga clic en **Ir**.
• Configure el número de versiones almacenadas en Panorama para una auditoría de configuraciones.	1. Seleccione **Panorama > Configuración > Gestión** y haga clic en el icono Editar en la sección Logs e informes. 2. Introduzca un valor entre 1 y 1048576 en **Número de versiones para auditoría de configuraciones**. El valor predeterminado es de 100. 3. Guarde los cambios. Haga clic en **Compilar** y seleccione **Panorama** como **Compilar tipo**.

VISTA PREVIA DE LOS CAMBIOS EN LA CONFIGURACIÓN	
• Vea y compare los archivos de configuración antes de compilar los cambios.	1. Seleccione **Compilar**. 2. Seleccione **Vista previa de cambios** y seleccione el número de líneas de contexto que le gustaría ver. 3. Haga clic en **ACEPTAR**.

Restricción de acceso a los cambios de configuración

Utilice los bloqueos para evitar que varios usuarios administrativos realicen cambios en la configuración o compilen cambios en Panorama, políticas compartidas o en plantillas o grupos de dispositivos seleccionados.

- ▲ Tipos de bloqueos
- ▲ Ubicaciones para aplicar un bloqueo
- ▲ Aplicación de un bloqueo
- ▲ Visualización de los portadores de bloqueo actuales
- ▲ Habilitación de la adquisición automática del bloqueo de compilación
- ▲ Eliminación de un bloqueo

Tipos de bloqueos

Hay dos tipos de bloqueos disponibles:

- **Bloqueo de configuración**: bloquea la realización de cambios en la configuración por otros administradores. Se puede establecer este tipo de bloqueo de forma general o para un sistema virtual. Solo puede eliminarse por el administrador que lo configuró o por un superusuario. El bloqueo de configuración no se elimina automáticamente.

- **Bloqueo de compilación**: Bloquea los cambios de compilación por parte de otros administradores hasta que se liberen todos los bloqueos. El bloque de compilación garantiza que los cambios parciales en la configuración no se compilen por error en el dispositivo o en Panorama cuando dos administradores están realizando cambios al mismo tiempo y el primer administrador acaba y compila los cambios antes de que el segundo haya terminado. El bloqueo se elimina automáticamente cuando el administrador que lo ha aplicado compila los cambios; el bloqueo lo puede eliminar manualmente el administrador que realizó el bloqueo o el superusuario.

  Si existe un bloqueo de compilación en un dispositivo y un administrador compila los cambios de configuración o políticas compartidas en una plantilla o grupo de dispositivos incluidos en ese dispositivo, la compilación fallará mostrando un mensaje de error que indica que hay un bloqueo activo en un dispositivo.



Los administradores de solo lectura que no pueden realizar cambios de configuración en el dispositivo o en Panorama no pueden aplicar ningún bloqueo.

Los administradores basados en función que no pueden compilar cambios pueden aplicar bloqueos de configuración y guardar los cambios en la configuración candidata. No pueden, sin embargo, compilar los cambios por sí mismos. Por esta razón, el bloqueo no se elimina automáticamente al compilar; el administrador debe eliminar el bloqueo de configuración manualmente después de realizar los cambios necesarios.

Ubicaciones para aplicar un bloqueo

El administrador puede aplicar un bloqueo en cualquiera de las siguientes categorías o *ubicaciones*:

- **Grupo de dispositivos**: restringe los cambios en el grupo de dispositivos seleccionado
- **Plantilla**: restringe los cambios en los dispositivos incluidos en la plantilla seleccionada
- **Compartido**: restringe los cambios en las políticas compartidas
- **Panorama**: restringe el acceso a los cambios en Panorama

Aplicación de un bloqueo

APLICACIÓN DE UN BLOQUEO	
Paso 1	Seleccione el icono de bloqueo en la esquina superior derecha de la interfaz web.
Paso 2	Seleccione **Tomar bloqueo**.
Paso 3	Basándose en su función/permisos, seleccione **Compilar** o **Configurar** como **Tipo**.
Paso 4	Seleccione la categoría en la que desea aplicar el bloqueo.
Paso 5	Se recomienda añadir un **comentario** para describir las razones de aplicar el bloqueo.
Paso 6	Haga clic en **ACEPTAR**.

Visualización de los portadores de bloqueo actuales

Antes de cambiar un área concreta de la configuración, compruebe si otro administrador ha aplicado un bloqueo en ella.

VISUALIZACIÓN DE LOS PORTADORES DE BLOQUEO

- Seleccione el icono de bloqueo en la esquina superior derecha de la interfaz web y vea los detalles.
  El icono de bloqueo muestra el número total de bloqueos aplicados. También incluye información sobre el nombre de usuario del portador del bloqueo, el tipo de bloqueo y la categoría en la que se ha realizado, cuándo se aplicó, la última actividad del administrador y si la sesión del administrador sigue o no activa.

Habilitación de la adquisición automática del bloqueo de compilación

De forma predeterminada, debe aplicar un bloqueo manualmente antes de empezar a hacer cambios en Panorama. Si desea habilitar la adquisición automática del bloqueo de compilación, siga estos pasos.

ADQUISICIÓN DE UN BLOQUEO DE COMPILACIÓN AUTOMÁTICO EN PANORAMA	
Paso 1	Seleccione la pestaña **Panorama > Configuración > Gestión** y haga clic en el icono Editar de la sección Configuración general.
Paso 2	Seleccione la casilla de verificación **Adquirir bloqueo de complicación automáticamente**.
Paso 3	Haga clic en **ACEPTAR**.
Paso 4	Para guardar los cambios, haga clic en **Compilar** y seleccione **Panorama** como **Compilar tipo**.

Eliminación de un bloqueo

ELIMINACIÓN DE UN BLOQUEO	
Paso 1	Seleccione el icono de bloqueo (1) en la esquina superior derecha de la interfaz web.
Paso 2	Seleccione el bloqueo que desea eliminar y haga clic en **Eliminar bloqueo**.
Nota	A no ser que sea un superusuario, solo puede eliminar un bloqueo que haya aplicado antes.
Paso 3	Haga clic en **ACEPTAR**.

Adición de logotipos personalizados

Puede cargar archivos de imágenes para personalizar las siguientes áreas de Panorama:

- Imagen de fondo en la pantalla de inicio de sesión
- Encabezado de la esquina superior izquierda de la interfaz web; también puede ocultar el fondo predeterminado de Panorama
- Página de título e imagen de pie de página en informes en PDF

Los tipos de imágenes compatibles incluyen los siguientes: .jpg, .gif y .png. Los archivos de imágenes para su uso en informes en PDF no pueden contener un canal alfa. El tamaño de la imagen debe ser inferior a 128 kilobytes (131.072 bytes); las dimensiones recomendadas aparecen en la pantalla. Si la dimensión es mayor que el tamaño recomendado, la imagen se recortará automáticamente.

ADICIÓN DE LOGOTIPOS PERSONALIZADOS

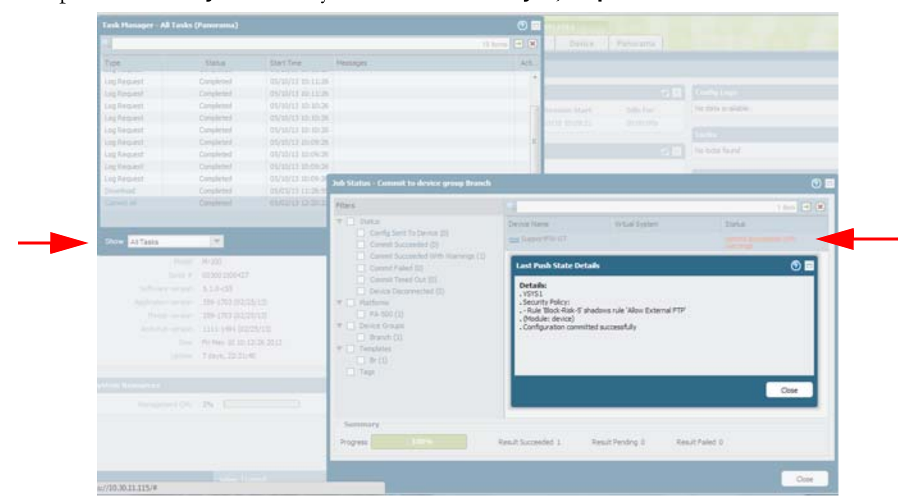
1. Seleccione **Panorama > Configuración > Operaciones**.
2. Haga clic en **Logotipos personalizados** en la sección Varios.
3. Haga clic en el icono Cargar logotipo y seleccione una imagen para cualquiera de las siguientes opciones: pantalla de inicio de sesión, esquina izquierda de la interfaz de usuario principal, página de título de informe en PDF y pie de página del informe en PDF.
4. Haga clic en **Abrir** para añadir la imagen. Para obtener una vista previa de la imagen, haga clic en el logotipo del icono de vista previa .
5. (Opcional) Para borrar el encabezado de fondo verde en la interfaz web de Panorama, seleccione la casilla de verificación **Remove Panorama background header (Eliminar encabezado de fondo de Panorama)**.
6. Haga clic en **Cerrar** para guardar los cambios.
7. Haga clic en **Compilar** y seleccione **Panorama** como **Compilar tipo**.

Visualización del historial de finalización de tareas

Los datos históricos sobre todas las tareas o tareas que se están ejecutando actualmente en Panorama se pueden ver usando el enlace **Tareas** en la interfaz web de Panorama. Muestra información sobre el éxito del evento e indica los errores, si hay alguno.

VISUALIZACIÓN DEL HISTORIAL DE TAREAS

1. Haga clic en **Tareas** Tasks. El enlace se muestra en la esquina inferior derecha de la interfaz web.
2. Seleccione la lista de tareas que se deben revisar. De forma predeterminada, aparece **Todas las tareas**. Puede filtrar por **Todos** o **Ejecutando** y seleccionar **Trabajos**, **Reports (Informes)** o **Peticiones de log**.



- Trabajos: indica las compilaciones, compilaciones automáticas, descargas e instalaciones de actualizaciones de software y dinámicas realizadas localmente en Panorama o transferidas de forma centralizada a los dispositivos gestionados desde Panorama. Cada trabajo es un enlace; haga clic en el enlace de la columna Tipo para ver los detalles de los dispositivos, el estado y revisar los errores, si los hay.
- Reports (Informes): muestra el estado y la hora de inicio de los informes programados.
- Peticiones de log: indica las consultas de logs activadas desde la pestaña **Supervisar >Visor de log** en el **Panel**. Por ejemplo, para mostrar los logs en el widget de filtrado de URL o de filtrado de datos en el Panel, se generan peticiones de log en Panorama.

Reasignación de cuotas de almacenamiento de logs

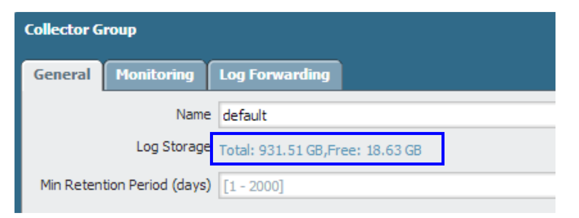
Para redistribuir la capacidad de almacenamiento de los logs disponibles en Panorama, puede aumentar o disminuir la cuota de almacenamiento de logs para cada tipo de log. El proceso de reasignación de cuotas de logs es distinto en el dispositivo virtual de Panorama y en el dispositivo M-100 en los siguientes aspectos:

- **En el dispositivo virtual de Panorama**: Todos los registros se escriben en el espacio de almacenamiento asignado al servidor: el disco de 10 GB predeterminado que se crea en la instalación o el disco virtual añadido al servidor, o la partición NFS que se monta en Panorama.
- **En el dispositivo M-100**: Los registros se guardan en dos ubicaciones: en el disco SSD interno y en los discos habilitados para RAID. El disco SSD interno del dispositivo M-100 se utiliza para almacenar los logs de configuración, los logs del sistema y las estadísticas de aplicación que Panorama recibe automáticamente en intervalos de 15 minutos desde todos los dispositivos gestionados. Todos los logs se almacenan en discos habilitados para RAID. Para volver a asignar la capacidad de almacenamiento para los logs almacenados en los discos RAID debe modificar la configuración del grupo de recopiladores.

Utilice las siguientes instrucciones para:

- Reasignar la cuota de almacenamiento de logs en el dispositivo virtual de Panorama
- Reasignar la capacidad de almacenamiento de logs para los logs del sistema, logs de configuración y estadísticas de la aplicación (Estadísticas de aplicación) en la dispositivo M-100
- Reasignar la capacidad de almacenamiento para los logs almacenados en los discos habilitados para RAID

REASIGNACIÓN DE LA CUOTA DE ALMACENAMIENTO DE LOGS EN EL DISPOSITIVO VIRTUAL DE PANORAMA Y DISPOSITIVO M-100	
Paso 1 Distribuya la capacidad de almacenamiento de los logs entre distintos tipos de logs. 	1. Seleccione **Panorama > Configuración > Gestión**. 2. Seleccione el icono de edición en la sección **Configuración de log e informes** de la pestaña **Gestión**. 3. Modifique la **cuota (%)** para los tipos de log en los que desea añadir o reducir el espacio de almacenamiento. Conforme cambia los valores, la pantalla se actualiza para mostrar el valor del número correspondiente (GB/MB) para el porcentaje asignado basado en el porcentaje total en el disco virtual/NFS/HDD, según corresponda. **Nota** En el dispositivo M-100, puede asignar la capacidad disponible entre los logs **Configurar**, **Sistema** y **Estadísticas de aplicación**; el resto de logs se escribe en los discos habilitados para RAID y no se almacenan en el HDD.

REASIGNACIÓN DE LA CUOTA DE ALMACENAMIENTO DE LOGS PARA LOS DISCOS HABILITADOS PARA RAID		
Paso 1	Asigne el porcentaje de capacidad de almacenamiento para cada tipo de log en el dispositivo M-100. Si la capacidad de almacenamiento de logs aparece como 0 MB, puede que no haya añadido el recopilador de logs al grupo de recopiladores. Complete el Paso 2 y, a continuación, vuelva a esta tarea. Si sigue indicando 0 MB, compruebe que los pares de discos se han habilitado para la creación de registros y que se han compilado los cambios en el grupo de recopiladores. Consulte el Paso 6 en la sección Adición de un recopilador de logs a Panorama.	1. Seleccione **Panorama > Grupos de recopiladores** y haga clic en el enlace del grupo de recopiladores. 2. Haga clic en el enlace de la capacidad **Almacenamiento de log** del grupo de recopiladores.  3. Modifique la **cuota** asignada a cada tipo de log. Conforme cambia los valores, la pantalla se actualiza para mostrar el valor del número correspondiente (GB/MB) para el porcentaje asignado basado en el porcentaje total en el grupo de recopiladores. 4. (Opcional) Haga clic en **Restablecer valores predeterminados** para deshacer los cambios y restablecer las cuotas a los valores predeterminados de fábrica, si es necesario.

Supervisión de Panorama

Puede configurar Panorama para que envíe notificaciones si se produce un evento del sistema o se realiza un cambio en la configuración en algún momento. De forma predeterminada, cualquier cambio en la configuración se registra en el log de configuración. En el log de sistema, los eventos aparecen con un nivel de gravedad asociado. El nivel indica la urgencia y el impacto del evento y puede elegir si desea registrar todos los eventos o solo eventos del sistema concretos según los niveles de gravedad que desea supervisar.



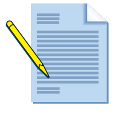
En esta sección solo se tratan los logs de Panorama. Para obtener información sobre cómo reenviar logs desde dispositivos gestionados, consulte Configuración de los cortafuegos para reenviar logs a Panorama.

- **Configuración**: permite el reenvío de logs de configuración especificando un perfil de servidor en los ajustes del log (**Panorama > Configuración de log > Configuración**).
- **Sistema**: permite el reenvío de logs del sistema especificando un perfil del servidor en los ajustes del log (**Panorama > Configuración de log > Sistema**). Seleccione un perfil de servidor para cada nivel de gravedad que desee reenviar. La siguiente tabla resume los niveles de gravedad de los logs de sistema:

Gravedad	Descripción
Crítico	Indica un fallo y señala la necesidad de atención inmediata, como un fallo de hardware, incluido el error de HA y los fallos de los enlaces.
Alto	Incidentes graves que afectarán al funcionamiento del sistema, incluida la desconexión de un recopilador de logs o un fallo de compilación.
Medio	Notificaciones de nivel medio, como actualizaciones del paquete antivirus o la compilación de un grupo de recopiladores.
Bajo	Notificaciones de menor gravedad, como cambios de contraseña de usuario.
Informativo	Eventos de notificación como inicio y finalización de la sesión, cambios en la configuración, realización correcta de la autenticación y notificaciones de fallo, realización correcta de la compilación y otros eventos no englobados en otros niveles de gravedad.

Los logs de configuración y del sistema se almacenan en el HDD del dispositivo M-100; en el dispositivo virtual de Panorama, se almacenan en el volumen de almacenamiento asignado. Si necesita el almacenamiento de logs con una mayor duración, para su auditoría, también puede configurar Panorama para que reenvíe los logs a un servidor Syslog.

Para supervisar Panorama, puede consultar los logs periódicamente en Panorama o configurar traps SNMP o alertas de correo electrónico que le notifiquen el cambio de estado de una métrica supervisada o cuando esta alcance un umbral Panorama. Las alertas de correo electrónico y traps SNMP son útiles para la notificación inmediata sobre eventos críticos del sistema que requieren su atención.



Panorama solo reenvía sus logs del sistema o de configuración generados localmente. No puede utilizar Panorama para reenviar logs enviados desde los dispositivos gestionados a un SIEM externo o servidor Syslog. No puede, por ejemplo, utilizar Panorama para reenviar logs de tráfico o amenazas a un servidor de almacenamiento externo.

Para configurar las alertas de correo electrónico y el acceso de SNMP, consulte las tareas siguientes:

- Configuración de alertas de correo electrónico
- Configuración del acceso SNMP

Configuración de alertas de correo electrónico

CONFIGURACIÓN DE ALERTAS DE CORREO ELECTRÓNICO	
Paso 1. Cree un perfil de servidor para su servidor de correo electrónico.	1. Seleccione **Panorama > Perfiles de servidor > Correo electrónico**. 2. Haga clic en **Añadir** y, a continuación, introduzca un **Nombre** para el perfil. 3. Haga clic en **Añadir** para añadir una nueva entrada de servidor de correo electrónico e introduzca la información necesaria para conectar con el servidor SMTP y enviar mensajes de correo electrónico (puede añadir hasta cuatro servidores de correo electrónico al perfil): • **Servidor**: nombre para identificar el servidor de correo electrónico (1-31 caracteres). Este campo es solamente una etiqueta y no tiene que ser el nombre de host de un servidor SMTP existente. • **Mostrar nombre**: el nombre que aparecerá el campo De del correo electrónico. • **De**: la dirección de correo electrónico desde la que se enviarán las notificaciones de correo electrónico. • **Para**: la dirección de correo electrónico a la que se enviarán las notificaciones de correo electrónico. • **Destinatarios adicionales**: si desea que las notificaciones se envíen a una segunda cuenta, introduzca la dirección adicional aquí. • **Puerta de enlace**: la dirección IP o el nombre de host de la puerta de enlace SMTP que se usará para enviar los mensajes de correo electrónico. 4. Haga clic en **Aceptar** para guardar el perfil de servidor.
Paso 2 (Opcional) Personalice el formato de los logs que envía Panorama.	Seleccione la ficha **Formato de log personalizado**. Si desea más información sobre cómo crear formatos personalizados para los distintos tipos de log, consulte Common Event Format Configuration Guide (Guía de configuración de formato de eventos comunes).

CONFIGURACIÓN DE ALERTAS DE CORREO ELECTRÓNICO (CONTINUACIÓN)		
Paso 3	Guarde el perfil de servidor y confirme los cambios.	1. Haga clic en **Aceptar** para guardar el perfil. 2. Haga clic en **Compilar** y seleccione **Panorama** como **Compilar tipo**.
Paso 4	Habilite la notificación de correo electrónico para eventos específicos del sistema y logs de configuración.	1. Habilite la notificación de correo electrónico. • Para eventos del sistema: a. Seleccione **Panorama > Configuración de log > Sistema**. b. Haga clic en el enlace de cada nivel de gravedad para el que desea habilitar la notificación y, a continuación, seleccione el perfil del servidor de correo electrónico creado en el Paso 1 del menú **Correo electrónico**. • Para cambios de configuración: a. Seleccione **Panorama > Configuración de log > Configuración**. b. Haga clic en el icono de edición de la sección Configuración de log - Configuración y, a continuación, seleccione el perfil del servidor de correo electrónico creado en el Paso 1 del menú **Correo electrónico**. 2. Haga clic en **Compilar** y seleccione **Panorama** como **Compilar tipo**.

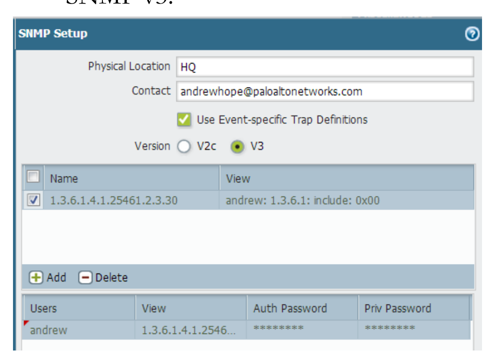
Configuración del acceso SNMP

El protocolo SNMP permite el acceso a identificadores de objetos (OID) específicos o intervalos de OID contenidos en la MIB de Palo Alto Networks desde una estación de gestión de SNMP. Se puede utilizar para consultar el estado de Panorama (GET de SNMP) y activar una alerta (trap SNMP) cuando se produce un evento. Panorama admite SNMP v2c y v3. Para ver una lista completa, consulte Palo Alto Networks MIBs (Bases de información de gestión de Palo Alto Networks).

Los traps SNMP alertan sobre un fallo o un cambio, como un fallo del ventilador del sistema, además de errores de HA o de las unidades de disco. Panorama inicia los traps y los envía al gestor de SNMP; no se envían con una frecuencia regular.

Los GET de SNMP permiten una supervisión proactiva. Puede, por ejemplo, sondear Panorama para buscar gráficos de tendencias que ayuden a identificar problemas potenciales del sistema antes de que se produzca un fallo en los siguientes ámbitos:

- Supervisión de la tasa de log entrante en un dispositivo M-100 o de la capacidad de los discos de registro en el dispositivo para determinar si un recopilador de logs se cierra al alcanzar su capacidad máxima. Esta información le ayudará a evaluar si necesita ampliar la capacidad de almacenamiento de los logs o añadir recopiladores de logs adicionales.
- Supervisión de la información del sistema como el modo de alta disponibilidad y el estado de Panorama o las versiones de actualización de contenido instaladas actualmente (versión del antivirus; versión de la base de datos de amenazas y aplicaciones o versión de Panorama).

CONFIGURACIÓN DE SNMP		
Paso 1	Configure la interfaz de gestión para escuchar al servicio de SNMP.	1. Seleccione **Panorama > Configuración > Gestión**. 2. En la sección Configuración de interfaz de gestión, compruebe que SNMP está habilitado en **Servicios**. Si SNMP no está habilitado, haga clic en el icono de edición de la sección Configuración de interfaz de gestión y seleccione la casilla de verificación del servicio **SNMP** y haga clic en **Aceptar** para guardar los cambios.
Paso 2	Configure Panorama para la supervisión de SNMP. Esta captura de pantalla pertenece a SNMP v3.  	1. Seleccione **Panorama > Configuración > Operaciones**. 2. En la sección Varios, seleccione **Configuración de SNMP**. 3. Introduzca una cadena de texto para especificar la **ubicación** física de Panorama. 4. Añada la dirección de correo electrónico de uno o varios **contactos** administrativos. 5. Seleccione la **versión** SNMP y, a continuación, introduzca los detalles de configuración de la siguiente forma (según la versión SNMP que utilice) y, a continuación, haga clic en **ACEPTAR**: • **V2c**: introduzca la **cadena de comunidad SNMP** que permita al gestor de SNMP acceder al agente de SNMP de Panorama. El valor predeterminado es **público**. Como se trata de una cadena de comunidad ampliamente conocida, es recomendable usar un valor que no se adivine tan fácilmente. • **V3**: debe crear al menos una vista y un usuario para poder utilizar SNMPv3. La vista especifica a qué información de gestión tiene acceso el gestor. Si desea permitir el acceso a toda la información de gestión, solo tiene que introducir el **OID** de nivel más alto de .1.3.6.1 y especificar la **opción** como **incluir** (también puede crear vistas que excluyan determinados objetos). Utilice **0xf0** como la **máscara**. A continuación, cuando cree un usuario, seleccione la **vista** que acaba de crear y especifique la **contraseña de autenticación** y la **contraseña privada**. La configuración de autenticación (la cadena de comunidad para V2c o el nombre de usuario y las contraseñas para V3) establecida en Panorama debe coincidir con los valores configurados en el gestor de SNMP. 6. Haga clic en ACEPTAR para guardar estos ajustes. 7. Haga clic en **Compilar** y seleccione **Panorama** en **Compilar tipo** para guardar los cambios en la configuración que se esté ejecutando.

CONFIGURACIÓN DE SNMP (CONTINUACIÓN)

Paso 3 Cree un perfil de servidor que contenga la información para conectarse y autenticar los gestores de SNMP.

1. Seleccione **Panorama > Perfiles de servidor > Trap SNMP**.
2. Haga clic en **Añadir** y, a continuación, introduzca un **Nombre** para el perfil.
3. Especifique la versión de SNMP que está usando (V2c o V3).
4. Haga clic en **Añadir** para añadir una nueva entrada de **receptor de trap SNMP** (puede añadir hasta cuatro receptores de traps por perfil de servidor). Los valores requeridos dependen de si está usando SNMP V2c o V3, como se explica a continuación:

   En SNMP V2c

   - **Servidor**: nombre para identificar el gestor de SNMP (1-31 caracteres). Este campo es solamente una etiqueta y no tiene que ser el nombre de host de un servidor SNMP existente.
   - **Gestor**: dirección IP del gestor de SNMP al que se envían los traps.
   - **Comunidad**: cadena de comunidad necesaria para autenticar en el gestor de SNMP.

   En SNMP V3

   - **Servidor**: nombre para identificar el gestor de SNMP (1-31 caracteres). Este campo es solamente una etiqueta y no tiene que ser el nombre de host de un servidor SNMP existente.
   - **Gestor**: dirección IP del gestor de SNMP al que se envían los traps.
   - **Usuario**: nombre de usuario necesario para autenticarse en el gestor de SNMP.
   - **EngineID**: ID del motor de Panorama. Es un valor hexadecimal de entre 5 y 64 bytes con un prefijo 0x. Cada Panorama tiene un ID de motor único. Para conocer el ID de motor, configure el servidor para SNMP v3 y envíe un mensaje GET desde el gestor de SNMP o el explorador de MIB a Panorama.
   - **Contraseña de autenticación**: contraseña que se usará para los mensajes de nivel authNoPriv para el gestor de SNMP. Esta contraseña contará con un algoritmo hash de seguridad (SHA-1), pero no estará cifrada.
   - **Contraseña priv.**: contraseña que se usará para los mensajes de nivel authPriv para el gestor de SNMP. Esta contraseña tendrá un algoritmo hash SHA y estará cifrada con el estándar de cifrado avanzado (AES 128).
5. Haga clic en **Aceptar** para guardar el perfil de servidor.

Paso 4	Habilite los traps SNMP para el log de configuración y los eventos de Syslog.	• Para eventos del sistema: a. Seleccione **Panorama > Configuración de log > Sistema**. b. Haga clic en el enlace de cada nivel de gravedad para el que desea habilitar la notificación y, a continuación, seleccione el perfil del servidor creado en el Paso 3 del menú **Trap SNMP**. • Para cambios de configuración: a. Seleccione **Panorama > Configuración de log > Configuración**. b. Haga clic en el icono de edición de la sección Configuración de log - Configuración y, a continuación, seleccione el perfil del servidor creado en el Paso 3 del menú **Trap SNMP**.
Paso 5	Guarde sus cambios.	Haga clic en **Compilar** y seleccione **Panorama** como **Compilar tipo**.

CONFIGURACIÓN DE SNMP (CONTINUACIÓN)		
Paso 6	Active el gestor de SNMP para interpretar las estadísticas un trap SNMP.	Para interpretar un trap enviado por Panorama, debe cargar los archivos MIB de PAN-OS en el software de gestión de SNMP y, si es necesario, compilarlos. Las MIB compiladas permiten al gestor de SNMP asignar el identificador de objeto (OID) a la definición del evento que define el trap Consulte las instrucciones específicas para realizar este proceso en la documentación de su gestor de SNMP.
Paso 7	Identifique las estadísticas que desea supervisar.	Use un explorador de MIB para examinar los archivos MIB de PAN-OS y localizar los identificadores de objeto (OID) que se corresponden con las estadísticas que desea supervisar. Por ejemplo, supongamos que desea supervisar la tasa de recopilación de logs en el dispositivo M-100. Usando un explorador de MIB verá que esta estadística se corresponde con los OID 1.3.6.1.4.1.25461.2.3.16.1.1.0 de PAN-LC-MIB.
Paso 8	Configure el software de gestión de SNMP para que supervise los OID que le interesan.	Consulte las instrucciones específicas para realizar este proceso en la documentación de su gestor de SNMP.

Reinicio o cierre de Panorama

La opción de reinicio activa la opción de reinicio correcto de Panorama. El cierre detiene el sistema y lo apaga. Para reiniciar Panorama, después de un cierre, desconecte y vuelva a conectar el cable de alimentación del sistema manualmente.

REINICIO/CIERRE	
Paso 1	Seleccione **Panorama > Configuración > Operaciones**.
Paso 2	En la sección Operaciones de dispositivo, elija una de las siguientes opciones: • Para reiniciar: Seleccione **Reboot Panorama (Reiniciar Panorama)**. • Para cerrar: Seleccione **Shutdown Panorama (Cerrar Panorama)**.

Generación de archivos de diagnóstico

Los archivos de diagnóstico facilitan la supervisión de la actividad del sistema y a detectar posibles problemas en Panorama. Para ayudar a los miembros de la asistencia técnica de Palo Alto Networks a solucionar problemas, el representante de la misma podría solicitarle los archivos de diagnóstico (archivo de asistencia técnica o de volcado de estadísticas). En el siguiente procedimiento se describe qué es un archivo de diagnóstico y cómo cargarlo en su caso de asistencia.

GENERACIÓN DE ARCHIVOS DE DIAGNÓSTICO
1. Seleccione **Panorama > Asistencia técnica**. • Haga clic en **Generar archivo de asistencia técnica**. • Haga clic en **Generar archivo de volcado de estadísticas**.
2. Descargue y guarde los archivos en el ordenador.
3. Cargue los archivos en su caso en el portal de asistencia técnica.

Configuración de perfiles de contraseña y complejidad de contraseña

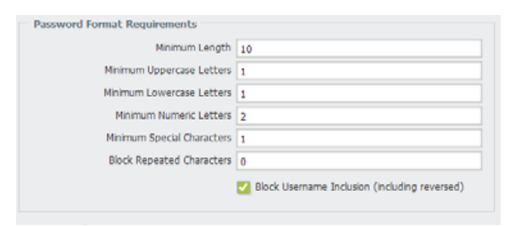
Para asegurar la cuenta del administrador local, puede definir los requisitos de complejidad de la contraseña que se aplican cuando los administradores cambian o crean nuevas contraseñas. Al contrario de lo que pasa en los perfiles de contraseñas, que se pueden aplicar a cuentas individuales, estas reglas de complejidad de contraseña se aplican a todo el dispositivo y a todas las contraseñas.

Para aplicar actualizaciones periódicas de la contraseña, cree un perfil de contraseña que defina un periodo de validez para las contraseñas.

PERFILES DE CONTRASEÑA Y AJUSTES DE COMPLEJIDAD

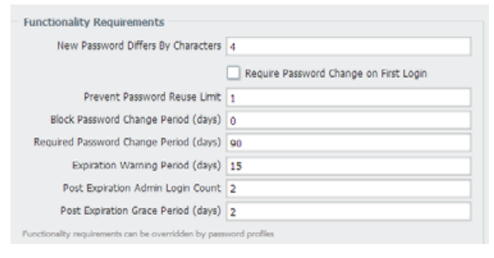
Paso 1 Configure ajustes de complejidad mínima de la contraseña.

1. Seleccione **Panorama > Configuración > Gestión** y, a continuación, haga clic en el icono Editar de la sección Complejidad de contraseña mínima.
2. Seleccione **Enabled (Habilitado)**.
3. Defina la opción **Requisitos de formato de la contraseña**. Puede aplicar los requisitos de formato que debe tener la contraseña (mayúscula, minúscula, números y caracteres especiales).
4. Para evitar que el nombre de usuario se utilice en la contraseña (o una versión invertida del nombre), seleccione **Bloquear inclusión de nombre de usuario (incluida su inversión)**.



5. Defina la contraseña **Requisitos de funcionalidad**.

   Si ha configurado un perfil de contraseña para un administrador, los valores definidos en el perfil de contraseña sobrescribirán los valores que ha definido en esta sección.



Paso 2 Cree perfiles de contraseña.

Puede crear varios perfiles de contraseña y aplicarlos a las cuentas de administrador según sea necesario para imponer la seguridad.

1. Seleccione **Panorama > Perfiles de la contraseña** y, a continuación, haga clic en **Añadir**.
2. Introduzca un **nombre** para el perfil de la contraseña y defina lo siguiente:
   a. **Período necesario para el cambio de contraseña**: frecuencia, en días, con la que deben cambiarse las contraseñas.
   b. **Período de advertencia de vencimiento**: días de antelación con los que el administrador recibirá un recordatorio de contraseña antes del vencimiento.
   c. **Período de gracia posterior al vencimiento:** número de días en los que el administrador puede seguir iniciando sesión en el sistema después del vencimiento de la contraseña.
   d. **Recuento de inicio de sesión de gestor posterior al vencimiento**: número de ocasiones en las que el administrador puede iniciar sesión en el sistema después del vencimiento de la contraseña.

Sustitución del disco virtual en un dispositivo virtual de Panorama

No se puede cambiar el tamaño de un disco virtual después de añadirlo a un dispositivo virtual de Panorama. Como el dispositivo virtual de Panorama solo permite una ubicación de almacenamiento de logs, si necesita añadir espacio en el disco para el registro (o disminuirlo, si había asignado más espacio), debe sustituir el disco virtual en el servidor ESX(i) para ajustar la capacidad de almacenamiento de logs.

Realice las siguientes tareas en el servidor ESX(i) para sustituir el disco virtual asignado a Panorama:

SUSTITUCIÓN DEL DISCO VIRTUAL ASIGNADO AL DISPOSITIVO VIRTUAL DE PANORAMA

Paso 1 Exporte los logs antes de desconectar el disco virtual del dispositivo virtual de Panorama. Dejará de poder accederse a los logs del disco después de desconectarlo.

1. Acceda a la CLI en el dispositivo virtual de Panorama y compruebe el uso del disco actual:

```
admin@Panorama> show system logdb-quota
```

2. Para exportar los logs, introduzca el comando:

```
admin@Panorama> scp export logdb to <cuenta de usuario>@<IP de servidor SCP>:
<ruta del directorio con nombre de archivo de destino>
```

Por ejemplo:

```
admin@Panorama> scp export logdb to sabel@10.236.10.30:/Panorama/log_file_exportMay2013
```

Nota Debe especificar un nombre de archivo; un archivo *.tar* con el nombre de archivo se guarda en el servidor SCP. Como los archivos se comprimen durante el proceso de exportación, el tamaño del archivo exportado será inferior al tamaño que tenía en el disco.

Paso 2 Desactive el dispositivo virtual de Panorama.

Paso 3 Edite la configuración en el dispositivo virtual de Panorama para añadir un nuevo disco virtual.

Paso 4 Cree un nuevo disco virtual con la capacidad deseada. El tipo de disco virtual debe ser IDE y la capacidad máxima 2 TB.



Paso 5 Elimine el disco virtual que desea sustituir.

Paso 6 Active el dispositivo virtual de Panorama. El proceso de reinicio podría llevar algunos minutos. En la pantalla, aparecerá un mensaje `cache data unavailable (datos en caché no disponibles)`.

Paso 7 Inicie sesión en el dispositivo virtual de Panorama.

Seleccione **Panorama > Configuración > Gestión**, compruebe que la capacidad de almacenamiento de logs aparece correctamente en la sección Logs e informes.



SUSTITUCIÓN DEL DISCO VIRTUAL ASIGNADO AL DISPOSITIVO VIRTUAL DE PANORAMA (CONTINUACIÓN)

Paso 8 Importe los logs al nuevo disco virtual en Panorama. Para importar los archivos al nuevo disco virtual, introduzca el siguiente comando de la CLI:

```
admin@Panorama> scp import logdb from <cuenta de usuario>@<IP de servidor SCP>: <ruta del directorio con nombre de archivo de destino>
```

7 Solución de problemas

Esta sección cubre los siguientes temas:

- ¿Por qué falla la compilación de plantillas?
- ¿Por qué ejecuta Panorama una comprobación de integridad del sistema de archivos?
- ¿Hay una conexión distinta para reenviar los logs a Panorama?
- ¿Por qué la capacidad de almacenamiento de logs del grupo de recopiladores indica 0 MB?
- ¿Por qué está Panorama en un estado suspendido?
- ¿Dónde puedo ver el estado de la tarea?

¿Por qué falla la compilación de plantillas?

La compilación de plantillas falla debido a las siguientes razones:

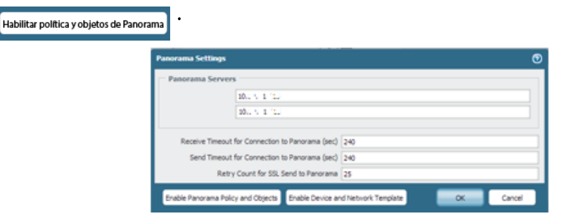
- Falta de coincidencia de las capacidades: Cuando se configura una plantilla, están disponibles las siguientes opciones: capacidad para varios sistemas virtuales, modo VPN y modo de operación.
  - Si está seleccionada la casilla de verificación para admitir varios sistemas virtuales, se producirá un fallo de compilación de plantilla cuando esta se aplique a los dispositivos que no puedan o no estén habilitados para la admitir varios sistemas virtuales.

    Para solucionar el error, edite la plantilla en la pestaña **Panorama > Plantillas** y deshabilite la casilla de verificación para **Sistemas virtuales**.
  - Si las opciones de configuración relacionadas con VPN se aplican a dispositivos diseñados para no permitir la configuración VPN.

    Para solucionar el error, edite la plantilla en la pestaña **Panorama > Plantillas** y habilite la casilla de verificación para **Modo de deshabilitación de VPN**.
  - Si el modo de operación habilitado en el dispositivo y el de la plantilla son diferentes. Por ejemplo, si el dispositivo gestionado está habilitado para el modo FIPS y la plantilla está definida para el modo normal.

    Para solucionar el error, edite la plantilla en la pestaña **Panorama > Plantillas** y compruebe que la selección de **Modo de operación** es la correcta.
- El dispositivo gestionado no está activado para recibir cambios de plantillas y de grupos de dispositivos de Panorama. Esto sucede cuando la capacidad de recibir cambios de configuración en las plantillas y en los grupos de dispositivos se ha deshabilitado en el cortafuegos.

Para solucionar el error, acceda a la interfaz web del dispositivo y seleccione **Dispositivo > Configuración**. Edite la sección Ajustes de Panorama y seleccione la casilla de verificación de **Habilitar plantillas de dispositivos y red** y **Habilitar política y objetos de Panorama**.



¿Por qué ejecuta Panorama una comprobación de integridad del sistema de archivos?

Panorama ejecuta periódicamente una comprobación de integridad del sistema de archivos (FSCK) para evitar daños en el sistema de archivos de Panorama. Esta comprobación se realiza cada 8 reinicios o tras un reinicio 90 días después de realizar la última comprobación de integridad del sistema de archivos (FSCK). Si Panorama ejecuta una FSCK, la interfaz web y las pantallas de inicio de sesión de SSH mostrarán una advertencia que indica que se está llevando a cabo una FSCK. No puede iniciar la sesión hasta que no finalice este proceso. El tiempo necesario para completar el proceso depende del tamaño del sistema de almacenamiento; dependiendo del tamaño, puede tardar varias horas en poder iniciar sesión en Panorama.

Para ver el progreso de la FSCK, configure el acceso de la consola a Panorama y consulte el estado.

¿Hay una conexión distinta para reenviar los logs a Panorama?

No, Panorama utiliza el puerto TCP 3978 para conectar a los cortafuegos.

En PAN-OS 4.x, la conexión SSL desde el cortafuegos a Panorama se realiza mediante un puerto TCP 3978. Se trata de una conexión bidireccional en la que los logs se reenvían desde el cortafuegos a Panorama; los cambios de configuración se aplican desde Panorama a los dispositivos gestionados. Los comandos de cambio de contexto se envían a través de la misma conexión.

En PAN-OS 5.0 y posteriores, y solo en una arquitectura de recopilación de logs distribuida con recopiladores de logs especializados, los cortafuegos gestionan dos conexiones SSL. Una conexión se destina a la gestión de Panorama y la otra al recopilador de logs. Ambas conexiones utilizan el mismo puerto: el puerto TCP 3978.

¿Por qué la capacidad de almacenamiento de logs del grupo de recopiladores indica 0 MB?

La capacidad de almacenamiento de logs del grupo de recopiladores podría indicar 0 MB si los pares de discos no están habilitados para los logs. Debe seleccionar el recopilador de logs y habilitar los pares de discos para los logs en la pestaña **Panorama > Recopiladores gestionados**; para obtener información, consulte el Paso 6 en la sección Adición de un recopilador de logs a Panorama.

Para comprobar que los discos están habilitados y disponibles para el almacenamiento de logs, seleccione la pestaña **Panorama > Recopiladores gestionados** y compruebe que el recopilador de logs aparece como **Conectado** y que el estado de configuración es **In sync (Sincronizado)**.

¿Por qué está Panorama en un estado suspendido?

Si Panorama está en un estado suspendido, compruebe lo siguiente:

- Compruebe que el número de serie de cada dispositivo virtual de Panorama es único. Si se utiliza el mismo número de serie para crear dos o más instancias de Panorama, se suspenderán todas las instancias que utilicen el mismo número de serie.
- Compruebe que ha establecido el ajuste de prioridad de HA en un peer como *principal* y el otro como *secundario*. Si el ajuste de prioridad es idéntico en ambos peers, el peer de Panorama con el número de serie más alto pasará al estado de suspensión.
- Compruebe que ambos peers de HA de Panorama están ejecutando la misma versión de Panorama (número de versión mayor y menor).

¿Dónde puedo ver el estado de la tarea?

Utilice el enlace Gestor de tareas en la esquina inferior derecha de la interfaz web de Panorama para ver si la tarea ha finalizado con éxito. También incluye un mensaje detallado que ayuda a depurar un problema. Para obtener más información, consulte Visualización del historial de finalización de tareas.